By Kyle W. Miller

The Increasing Need for Consumer Privacy Ombudsmen

Kyle W. Miller
Dentons
Louisville, Ky.

Kyle Miller is a partner in Dentons' global Data Privacy and Cybersecurity Group in Louisville, Ky. He has built his career as a cybersecurity professional in assisting clients with needs related to cybersecurity, data-privacy and technology, and he has experience facilitating data-governance concerns for the sales of businesses and assets.

The consumer privacy ombudsman (CPO) became part of the Bankruptcy Code via the Bankruptcy Abuse Prevention and Consumer Protection Act of 2005 (BAPCPA). Two decades ago, the regulatory and legal landscape was markedly different than it is today. The primary enforcer of privacy rules in 2005 was the Federal Trade Commission (FTC), which was limited to its enforcement powers under § 5 of the FTC Act of 1914 to bringing actions for unfair or deceptive acts or practices in interstate commerce.[1] Absent clear rules about what constitutes a privacy violation, the FTC would hold companies accountable for violating the notice requirements when the data was collected.[2] With few other protections to reference, the Code was amended as follows:

> The trustee, after notice and a hearing, may use, sell, or lease, other than in the ordinary course of business, property of the estate, except that if the debtor in connection with offering a product or a service discloses to an individual a policy prohibiting the transfer of personally identifiable information about individuals to persons that are not affiliated with the debtor and if such policy is in effect on the date of the commencement of the case, then the trustee may not sell or lease personally identifiable information to any person unless —
>
> (A) such sale or such lease is consistent with such policy; or
>
> (B) after appointment of a consumer privacy ombudsman in accordance with section 332, and after notice and a hearing, the court approves such sale or such lease —
>
> (i) giving due consideration to the facts, circumstances, and conditions of such sale or such lease; and
>
> (ii) finding that no showing was made that such sale or such lease would violate applicable nonbankruptcy law.[3]

Prior to the dot-com boom and subsequent bust, companies made blanket assertions about not selling identifiable data. Now, the blanket statement that personal data will be transferred to subsequent parties-in-interest in the event of an asset sale, stock sale, change in control or pursuant to a bankruptcy proceeding is found in virtually every online privacy notice. Bankruptcy courts might construe these simple declarations that a user's data could be transferred or sold in a bankruptcy proceeding as evidence that such a sale would not violate the privacy notice and therefore see no need to appoint a CPO under § 363. However, such an approach would miss the important changes in the privacy landscape that have been made since BAPCPA was implemented.

Consumer Expectations and Rights Have Changed Significantly Since 2005

Eleven years after the passage of BAPCPA, the EU enacted the General Data Protection Regulation (GDPR), which marked a sea change in how individuals expect their data to be handled around the world.[4] U.S. laws at the time narrowly regulated specific types of data in the hands of specific types of entities, such as genetic data possessed by insurance companies under the Genetic Information Nondiscrimination Act of 2008,[5] or protected health information in the hands of certain medical companies under the Health Insurance Portability and Accountability Act of 1996.[6] The Bankruptcy Code limits the definition of "personally identifiable information" to an individual's name, home address, email address, home phone number, Social Security number or credit card number.[7]

On the other hand, the GDPR defined "personal data" as "any information relating to an identified or identifiable natural person"[8] and placed strict requirements and limits on how companies could process such personal data. Thirteen years

1 15 U.S.C. § 45(a)(1)-(2).
2 *FTC v. Toysmart.com LLC*, No. 00-11341, 2000 WL 34016434, at *1 (D. Mass. July 21, 2000).
3 11 U.S.C. § 363(b)(1).
4 Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.
5 42 U.S.C. § 2000ff.
6 45 C.F.R. § 160.103.
7 11 U.S.C. § 101(41A).
8 General Data Protection Regulation Art. 4(1).

continued on page 51

after BAPCPA's passage, California passed the California Consumer Privacy Act (CCPA). Similar to the GDPR, the CCPA defines "personal information" as "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[9] The CCPA approach to regulating the processing of data under a broad definition is referred to as a "comprehensive" privacy law, as opposed to the laws with more limited definitions, such as state data-breach notification laws or the Bankruptcy Code. As of March 2025, 19 states have passed similar "comprehensive" privacy laws with a broad definition of "personal information," and give individuals in those states specific rights over their data.[10]

The Devil Is in the Details

While many of the state comprehensive laws are extremely similar, they also have meaningful nuances that will affect an individual's rights and a company's obligations. Restructuring professionals are adept at selling assets, but what constitutes a "sale" of personally identifiable data under state comprehensive laws varies. Some states define the sale of personal data as "the exchange of personal data for monetary consideration by a controller to a third party."[11] However, other states define a sale as the "exchange of personal data for monetary *or other valuable consideration* by the controller to a third party."[12] This distinction is critical in practice.

For example, in *People v. Sephora United States*, the California Attorney General alleged that Sephora sold data in violation of the CCPA by using common advertising and analytics technology on its website.[13] Although Sephora did not necessarily pay for the analytics services, the fact that it transferred data to an analytics company, then received "higher quality analytics" in return, was sufficient valuable consideration to be deemed a sale of personal information.[14] Sephora ultimately agreed to a $1.2 million settlement and injunctive relief.[15]

Determining what state or federal law applies to a company is not always straightforward. A state's comprehensive laws have their own thresholds for applicability depending on the company's size,[16] the amount of personal data that it processes[17] or how it profits from personal data.[18] These comprehensive laws also have exemptions for applicability so as to not overlap with other privacy regimes. Again, though, these exemptions are not universally applied.

The majority of state comprehensive consumer-privacy laws provide exemptions to both financial institutions and affiliates of financial institutions[19] regulated by the Gramm-Leach-Bliley Act (GLBA) from obligations under these privacy laws, but a minority do not. For example, Minnesota only provides the exemption to affiliates or subsidiaries of insurers that are "principally engaged in financial activities, as described in United States Code, title 12, section 1843(k)," such as bank-holding companies;[20] on the other hand, Connecticut, New Hampshire, Oregon, Texas and Virginia do not exempt "affiliates" at all;[21] and California does not provide an entity exemption to begin with — only exempting the "data" subject to the GLBA.[22] Therefore, in at least seven states, the state comprehensive consumer-privacy laws might be enforceable against the non-GLBA affiliate.

On Jan. 13, 2025, the Texas Attorney General brought an action against six affiliated defendants alleging violations of the Texas comprehensive privacy law and other state laws.[23] According to the complaint, three of the defendants are insurance companies regulated by state equivalents of the GLBA, but the remaining three defendants are wholly owned subsidiaries of insurance companies that primarily engage in data analytics and are not regulated under the GLBA. As Texas does not have an affiliate exemption, the subsidiary entities are arguably governed by the Texas comprehensive laws, even though their parent company is not.

The comprehensive laws also have heightened requirements for processing "sensitive information" but have differences in determining exactly what sorts of information fall into that definition. Most will include geolocation data, children's data, health data or sexual-orientation information.[24] However, California uniquely includes philosophical beliefs,[25] Oregon and Connecticut include status as a victim of a crime,[26] and Maryland and Oregon include national origin.[27]

These regulations are rapidly changing as more states consider and pass their own comprehensive laws and the enacted laws are amended. It is impossible to know whether a sale of data violates privacy notice requirements without knowing these laws and monitoring their evolution.

9 Cal. Civ. Code § 1798.140(v)(1).
10 Specifically, California, Colorado, Connecticut, Delaware, Indiana, Iowa, Kentucky, Maryland, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, Oregon, Rhode Island, Tennessee, Texas, Utah and Virginia.
11 *See, e.g.*, Ind. Code 24-15-2-27(a).
12 *See, e.g.*, Cal. Civ. Code 1798.140(ad)(1); Colo. Rev. Stat. § 6-1-1303(23); Conn Gen. Stat. § 42-515(26); Tenn. Code 47-18-3301(24); Texas Code 11-541.001(28).
13 *People v. Sephora USA Inc.*, No. CGC-22-601380 (Cal. Super. Aug. 24, 2022), Compl. ¶ 2.
14 *Id.* at ¶ 13.
15 *People v. Sephora USA Inc.*, No. CGC-22-601380, 2022 WL 22913962, at *2 (Cal. Super. Aug. 24, 2022).
16 Tex. Bus. & Com. Code Ann. § 541.002(a)(3).
17 Iowa Code Ann. § 715D.2(1)(b).
18 *Id.*
19 Colorado (Colo. Rev. Stat. § 6-1-1304(2)(q)), Delaware (Del. Code tit. 6, § 12D-103(b)(2)), Indiana (Ind. Code § 24-15-1-1(b)(2)), Iowa (Iowa Code § 715D.2(2)), Kentucky (Ky. Rev. Stat. § 367.3613(2)(b)), Maryland (Md. Code, Com. Law § 14-4703(a)(3)), Montana (Mont. Code § 30-14-2804(1)(e)), Nebraska (Neb. Rev. Stat. § 87-1103(2)(b)), Rhode Island (6 R.I. Gen. Laws § 6-48.1-10(a)), Tennessee (Tenn. Code § 47-18-3311(a)(2)), and Utah (Utah Code § 13-61-102(2)(k)).
20 Minn. Stat. § 325M.12(2)(18).
21 Cal. Civ. Code § 1798.145(e)); Conn. Gen. Stat. § 42-517(a); N.H. Rev. Stat. § 507-H:3(I)(e); Ore. Rev. Stat. Ann. § 646A.572(2)(L); Tex. Bus. & Com. Code Ann. § 541.002(b)(2); Va. Code § 59.1-576(A).
22 Cal. Civ. Code 1798.145(e).
23 *Texas v. Allstate Corp., et al.*, Docket No. 25-01-00561 (Tex. Dist. Ct. Jan. 13, 2025).
24 *See, e.g.*, Tenn. Code Ann. § 47-18-3302(26).
25 Cal. Civ. Code § 1798.140(ae)(D).
26 Ore. Rev. Stat. Ann. § 646A.570(18)(a); Conn. Gen. Stat. Ann. § 42-515(38).
27 Md. Code Ann., Com. Law § 14-4707(a)(7); Ore. Rev. Stat. Ann. § 646A.570(18)(a).

continued on page 52

Cyber-U: The Increasing Need for Consumer Privacy Ombudsmen

from page 51

When to Consider a CPO

These newer regulations do not necessarily mean that a CPO must be appointed in every instance where a debtor processes personal information. However, additional thought should be given in certain circumstances.

First, consider a CPO's assistance when the debtor is a "controller" of consumer data. The term "controller" is utilized by the GDPR, and nearly all state comprehensive laws[28] refer to the entity that determines the purpose and means of processing personal data. Put another way, the controller sets the terms of the initial processing. Many other companies will process data on the controller's behalf, but those companies will be considered processors, service providers, contractors or vendors. When these entities process data in violation of the controller's terms, the controller likely has a breach-of-contract claim to cure those violations. When such an entity enters bankruptcy, the controllers might enter the action to enforce their rights over the consumer data, but when a controller is in the bankruptcy process, only consumers would have rights to assert over the subsequent transfer of their data.

Second, consider the assistance of a CPO when the debtor has a significant volume of data. The state comprehensive privacy laws routinely exclude small businesses, only seeking to regulate companies that have many records.[29] In addition, some of the state comprehensive laws limit the amount of data that may be processed. For example, in Maryland, controllers may only collect data "reasonably necessary and proportionate to provide or maintain a specific product or service requested by the consumer to whom the data pertains."[30] Under those laws where data-minimization standards are important, there will be the question of whether the data set to be sold should have been processed in the first place.

Third, consider the assistance of a CPO when the debtor processes information that might be considered "sensitive." Although state definitions vary, bankruptcy courts can realize the particular risk of harm to individuals when particular data elements are transferred to third parties. While every comprehensive privacy law includes some variation of geolocation information in its definition of "sensitive data," geolocation that relates to (or could reasonably infer) other sensitive data, such as an individual's medical providers, religious beliefs, trade union membership, political beliefs, sexual orientation or ethnicity, might get heightened scrutiny.[31]

Conclusion

Although § 363 of the Bankruptcy Code contemplates appointing a CPO when a sale of data would violate the debtor's privacy notice requirements, a CPO is valuable to evaluate that threshold question and explain the applicability of many other restrictions on transferring data that did not exist when BAPCPA was enacted. Section 105(a) gives bankruptcy courts broad discretion to raise issues on its own motion, and, as in other areas of the Code, the court can call on privacy professionals to assist when needed.[32]

This was likely Congress's intent when it passed BAPCPA. In discussing potential amendments to the privacy protections of the Bankruptcy Code in 2005, then-Sen. Patrick Leahy (D-Vt.) asserted that bankruptcy courts "are in a unique position to properly balance the need to share information with the need to protect privacy, and we should rely on their good judgment and discretion as much as possible."[33] Although bankruptcy courts might not immediately know whether a sale of data is in violation of a privacy notice requirements without understanding the nuances of the laws that have emerged since 2005, the CPO could be relied on to ensure that individuals' rights are not ignored. abi

28 California is unique in referring to such entities as "businesses."

29 *See, e.g.*, Conn. Gen. Stat. § 42-516. (applying act only to businesses that "(1) Controlled or processed the personal data of not less than [100,000] consumers, excluding personal data controlled or processed solely for the purpose of completing a payment transaction; or (2) controlled or processed the personal data of not less than [25,000] consumers and derived more than [25 percent] of their gross revenue from the sale of personal data").

30 Md. Code Ann., Com. Law § 14-4707(b)(1)(i).

31 In particular, "information about visits to or stays at the following locations: medical facilities, religious organizations, correctional facilities, labor union offices, locations providing services to LGBTQ+ individuals, locations of political demonstrations, locations providing education or childcare to minors, racial or ethnic organizations, locations providing shelter or social services, and military installations, offices, or buildings" is considered "sensitive." *See* Bhavna Changrani, "Protecting Consumers' Location Data: Key Takeaways from Four Recent Cases," *Compliance & Enforcement*, wp.nyu.edu/compliance_enforcement/2024/12/05/protecting-consumers-location-data-key-takeaways-from-four-recent-cases (last visited on March 31, 2025).

32 3 *Collier on Bankruptcy* ¶ 332.02 (16th 2025) ("Bankruptcy courts often expand upon a statutory authorization such as section 332 to order the appointment of officers or professionals at the expense of the estate when the court feels that it could benefit from the additional information or assistance that a neutral third party might provide.").

33 151 Cong Rec. S. 1726, 1782.