Privacy Issues in Business Combinations

By **Dominique Shelton Leipzig** and **G. Thomas Stromberg**, Partners at Perkins Coie

Every buyer of a U.S. business needs to think about what liabilities it is acquiring in the transaction and how to minimize or eliminate those liabilities or to become comfortable with the liabilities. Some liabilities are easily known (secured debt, major contracts, and real property leases), while other liabilities are not as obvious (environmental liabilities, unasserted claims, liens that do not show up in a central filing, and, increasingly, data). Specifically, one potential liability that has recently become significant is failure of an acquired business to comply with applicable privacy laws. Recent legislation, particularly in California, has made a compliance program essential for qualifying businesses, and failure to have a compliance program can result in significant liability, which a buyer should know about and plan for.

It is important to understand the applicable regulatory regimes pertaining to privacy when acquiring a business. In international acquisitions, much has been made of the EU General Data Protection Regulation (GDPR) as a game changer for privacy. Similar laws are now becoming part of the U.S. landscape. Ifthe target company is based in California or does business in California, the buyer (whether a U.S. entity or non-U.S. entity) needs to understand when the California Consumer Privacy Act (CCPA) will apply.

The CCPA covers any “business”(whether or not located or incorporated in California) that collects personal information (PI) from California residents. The term “business” is defined in the CCPA to have extraterritorial effect and will apply to any business that collects PI if one of three things also occurs:

1. The business has revenues of over $25 million; or
2. The business collects PI of 50,000 California residents or more; or
3. The business derives 50% or more of its revenue from the sale of California data.

Please note that the CCPA includes a very broad definition of PI. It is broader than the definition of PI in the EU’s GDPR because it includes not only data types such as cookie

data, unique device identifiers, names, emails, addresses, and phone numbers but also *inferences* drawn from the preceding.

For a buyer of a business that, according to the requirements set out above, is subject to the CCPA, it is essential to determine whether the target company is in compliance with the CCPA. If the target company is not in compliance with the CCPA and the non-compliant company is purchased, then the buyer could be liable for up to $7500 per violation if enforced by the California Attorney General and $750 per violation if a consumer pursues a class action. Put another way, if a website has 1 million California visitors per year and the privacy policy is not in compliance, the California Attorney General can set fines for each separate violation every time California residents visit that website up to US$7,500,000,000.

While the requirements of the CCPA are intricate and technical, at the core of complying with the CCPA is knowing how to deal with consumers' requests with respect to any of the eight rights regarding their PI. These rights are:

- An abbreviated right to disclosure of specific pieces and categories of PI collected.
- An expanded right that mirrors the abbreviated right to know and adds information regarding the sources and disclosure of PI collected.
- Right to disclosure regarding PI sold or disclosed for a business purpose.
- Right to optout of the sale of PI.
- Right to optin for the sale of a minor's PI.
- Right to deletion of PI collected.
- Right to access PI.
- Right to not be discriminated against.

A business must provide at least two designated methods, including a toll-free telephone number and a website address (if it has a website), for consumers to submit the requests. Companies with websites should take care to ensure that requests made through the website are routed to a centralized location and that the person responding to the requests is properly trained on how to do so. We have seen companies that failed to do this have problems complying with consumer requests made under the GDPR, either by leaving some requests unaddressed or by addressing them in inconsistent ways, opening themselves up to regulatory investigation.

If a buyer determines that a company it proposes to acquire is not in compliance with the CCPA, the buyer may want to require the target to come into compliance before the transaction closes or may want to complete the acquisition and bring the acquired company into compliance after closing of the acquisition. In either case, it is important to know how best to create a privacy program that includes the systems and policies to comply. Please note that each business that is subject to the CCPA must establish procedures to implement obligations relating to consumer rights in time for the effective date of the CCPA on January 1, 2020.

In creating a privacy program, it is important to look ahead and think strategically about who the company's audience might be. At the outset, a business needs to implement systems to ensure that consumer requests are "verifiable"—that is, the consumer himself or herself is making the request. The CCPA does not specify exactly how a business should verify a consumer request and indicates that the California Attorney General's Office should adopt regulations specifying how to do so. Given that the regulations may not be adopted soon enough for businesses to be able to operationalize them prior to the effective date of January 1, 2020, businesses should consider implementing methods, such as two-factor authentication and blockchain technology, now. In that case, come January 1, 2020, they can be reasonably confident that they are not disclosing or delivering PI to someone other than the person to whom the PI belongs. If a request is not verifiable, then the business should not disclose the PI.

There are other reasons why PI need not (or should not) be disclosed or delivered. For example, a business need not or should not disclose PI if the individual has submitted rights requests more than twice in the preceding 12-month period, if a request relates to PI collected more than 12 months prior, or if fulfilling the request would infringe the rights and freedoms of other individuals. Once a business verifies the request and determines that no defenses apply, it should know exactly what it is obligated to produce, and the response needs to satisfy the CCPA's requirements regarding the method and timing of delivery. This means that the business should respond within 45 days unless unusual circumstances exist, in which case an additional 90-day extension can be obtained. Further, the responses should detail the specific pieces of PI collected about the consumer to respond to an access request or the right to know about data collected, sold or disclosed for a business purpose.

In addition, a company needs to structure its privacy program so that it will pass the scrutiny of regulators and judges resulting from a lawsuit, unwanted publicity, or data

breach. It is critical to be able to demonstrate that the privacy program substantially complies with the requirements of the CCPA. This can be accomplished by developing privacy programs that follow guidance promulgated by regulators and courts. This guidance includes the CNIL's (the French Data Protection Authority's) Six Steps for GDPR Compliance, along with Federal Trade Commission orders such as the Vizio 2017 order, which provide a roadmap for a comprehensive privacy program that can be distilled down to six main phases:

Phase 1: Appoint at least one leader/task force to lead the privacy program.

Phase 2: Inventory data assets and flows. Consider using CNIL's data inventory template form.

Phase 3: Conduct a gap analysis/risk assessment by benchmarking practices identified in Phase 2 with the applicable legal requirements.

Phase 4: Conduct a data impact assessment for high-risk processing (e.g., data flows associated with children as well as medical, financial, or location data).

Phase 5: Mitigate risks identified in Phases 3 and 4 by implementing appropriate policies and procedures to govern data practices, including internal governance policies and procedures, external-facing policies (e.g., website, mobile app), vendor management policies, and employee training.

Phase 6: Create an auditable record to demonstrate compliance.

By using this roadmap, businesses can streamline compliance efforts, reduce their exposure to litigation and enforcement, and present a defensible position if faced with such a situation relating to a company that they acquire.

Conclusion: Many U.S. businesses are required to comply with applicable privacy laws and regulations. Among these laws and regulations is the CCPA, which has been adopted by the California legislature and goes into effect on January 1, 2020. The CCPA has broad application, and many businesses located in California or doing business in California will be required to comply. If a business is required to comply with privacy laws such as the CCPA and does not, it can face exorbitant fines of up to $7500 per violation imposed by the California Attorney General. In addition, the CCPA gives California residents the right to bring privacy class actions, whereby they could seek $750 per breached Califor-

nia record. Based upon the number of breaches that were posted on the California Attorney General's website, this would represent a collective $37 billion exposure for companies. Any buyer (U.S. or non-U.S.) of a U.S. business should determine (i) whether privacy laws such as the CCPA apply to the target business, (ii) if privacy laws such as the CCPA do apply, whether the target business is in compliance with the applicable privacy laws,and (iii) if the target is not in compliance, whether the buyer wants to require the target business to comply before closing, bring the target company into compliance after closing, or not complete the transaction.

If a buyer or business owner decides to implement a privacy program, the program should provide (i) a method of verifying a consumer request, (ii) a method of handling consumer requests pertaining to the eight rights regarding PI (listed above), and (iii) other methods geared to show compliance that regulators and courts have determined and stated to be important for compliance with applicable laws.