Don't Let Privacy Issues Tank Your Data-driven M&A Deal - a blog post by Michael Whitener

More and more M&A transactions are “data driven” – meaning data is central to the deal’s value. But if acquirers are not careful, they could find themselves saddled with serious privacy and data security issues post-acquisition. The once-coveted target company could turn out to be an albatross.

At one level, privacy and data security are simply legal compliance issues. Is the target company aware of what privacy/data protection laws apply to it, and has it consistently posted and maintained a compliant privacy policy? Has the target company implemented commercially reasonable data security policies? Has the target company ever suffered a data security breach, and if so, how did the company respond?

Increasingly, however, privacy issues are at the core of the value of data-driven businesses. The goodwill – and ultimately the value – of these businesses is integrally tied to how fairly and transparently they handle the personal data of their customers and partners. In this scenario, any questionable privacy practices of a target company may be a deal breaker.

Examination of a target company’s privacy-related policies and practices should be considered “pre-diligence” in data-driven deals. Even before beginning to negotiate a stock or asset purchase agreement, see if there are any red flags from a privacy or security perspective. If the red flags are significant, the deal could be dead on arrival.

Imagine a scenario in which a prime asset of the target company is its customer list. The acquirer bids high for the target company, anticipating the profits to be gleaned from marketing to the target company’s customers.

But wait – the target company’s privacy policy says: “We will never sell your data.” There’s no exception for a merger or acquisition. Furthermore, the target company’s customer agreements don’t permit any use of customer data except to provide services to the customers. No other marketing uses are permitted.

The target company offers to revise its privacy policy, which the privacy policy (by its terms) permits. But as the Federal Trade Commission has made clear, you can’t retroactively apply a revised privacy policy to personal data collected before the revisions went into effect.

In addition, if the target company has been out of compliance with the GDPR, the CCPA, HIPAA, COPPA, GLBA, and the rest of the alphabet soup of privacy laws, the acquiring company will simply inherit this headache of bringing the target into compliance – and dealing with any liability that may have arisen pre-acquisition.

The acquiring company might argue: “Well, we’ll deal with these issues in the representations and warranties and indemnification sections of the acquisition agreement.” While this approach might provide a financial safety net, it doesn’t resolve the underlying issues. As an acquirer, don’t you want to know the reality of what privacy/security time bombs you may be taking on?

Here’s a more common-sense approach. *First*, conduct thorough “pre-diligence.” Get the answers from the target company to such questions as:

1. What personal data do you collect, from what sources, and how is such personal data stored, processed, transferred and retained?
2. Does your privacy policy fully cover such personal data processing? And does it permit transfer of such personal data to the acquirer? Please provide current and historical copies.
3. Have you carefully considered what privacy/data protection laws apply to your processing of personal data? Are you confident you’re in full compliance?
4. What are your data security practices and protocols? Do you have both a written information security plan and a security incident response plan?
5. Do you conduct periodic privacy and/or data security assessments or audits? Please provide results.
6. Have you ever experienced a data security breach? If so, provide details.
7. Have you ever received a complaint or a governmental inquiry regarding your data security or privacy practices?
8. Do you provide employee training with regard to privacy and security compliance?

Second, consider requiring the target company to take remedial measures to clean up any privacy/security deficiencies before closing. For instance, fixes to the target’s privacy policy, amendments to the target’s key customer and supplier agreements, and revamping of the target’s data protection agreements and other privacy-related templates may be in order.

Inevitably, privacy issues will increase in prominence in M&A transactions. The best practice is to get a handle on them at the outset of a proposed acquisition so they don’t haunt the parties down the road.