

PRIVACY IN M&A – Personal Information has moved up to the Grown-up Table

Whether you are the seller or the buyer, corporate privacy policies included in the companies' websites have an enormous impact on a future merger or acquisition. From the perspectives of required due diligence, warranties and even whether the transaction may proceed at all, companies must think carefully about their (or their targets') data practices at the time of collection of the personal information (PI).

One need only recall the Radio Shack bankruptcy, where due to its privacy policy statements, Radio Shack was required to destroy much of the PI it owned rather than transfer it to the buyer of its assets. Even outside bankruptcy, prospective buyers and sellers must be aware of the implications of this situation and the resulting accord among state Attorneys General (the "Radio Shack Accord").

Internal and external due diligence on your (and your targets') data practices and policies is therefore advised before contemplating a merger or acquisition (and making or requesting particular representations and warranties about the PI). Data collected in a moment of time is "attached" to the privacy policy that is in place at such time of collection. We advise that you organize your PI according to the applicable privacy policy version in place at the time of collection, and for each set (if more than one policy), analyze the following, depending on whether you are buying or selling:

1. Did the policy specifically contemplate a transfer of the user's PI in the context of a change of control? This is the primary lesson to be learned from Radio Shack. If the policy makes a blanket statement without exception that PI will not be sold, then you have a problem that needs addressing. While a policy may be revised, users must have consented to that change (see below) before placing their PI in the "transferable upon change of control" bucket.
2. Is PI a material element of the value of the deal?
3. Does the policy specifically get the user's consent to *prospective* changes to privacy policies? Perhaps more importantly, does the prospective policy apply with respect to the data collected at such earlier time? Data collected from the former policy cannot be "upped" without user consent.
4. What does the privacy policy say about notifying users of policy changes and the manner of notification?
5. Does the policy provide that continued activity or provision of PI constitutes consent?
6. How was user consent obtained to the original privacy policy? There is developing case law that calls into question "passive" methods by websites and mobile apps of obtaining a user's consent. If a user did not affirmatively take action to indicate consent after having an opportunity to read the policy and terms, there may be questions as to enforceability. Renewed affirmative consent is advised.
7. If PI is material, what does the Radio Shack Accord dictate for the transaction?
8. What sort of warranties regarding seller compliance with its policy are possible and necessary?
9. What is a reasonable way to allocate in the indemnification section, the risk of private or governmental challenges to privacy practices?
10. For deals with a material non-US element, it is necessary to conduct this type of review with respect to data collection in each of the locations in which users reside.

FISHERBROYLES[®]

A LIMITED LIABILITY PARTNERSHIP

As for the acquisition or merger agreement, typical representations and warranties include the following (which may include knowledge or materiality qualifiers and international and industry considerations):

- (i) **Company complies with its published privacy policies.** Privacy policies need to reflect actual practice as it changes from time to time.
- (ii) **Company complies with privacy and data security laws and regulations.** This representation includes rules applicable to specific industries (financial, health care). We are seeing unduly vague terms such as “guidance” or “industry standards” in written agreements. Exact terms and specificity should be used whenever possible..
- (iii) **The acquiring entity will comply with the sellers’ published policy.**
- (iv) **The Company has in place commercially reasonable (or industry standard) privacy and data security practices.** This provision packs in quite a lot: encryption, firewalls, patch deployment, access restrictions, incident response preparedness, penetration testing, physical security, policies regarding use of personal devices, cyber insurance, etc. It may be preferable for both sides to address compliance with recognized standards.
- (v) **There has been no data breach or privacy violation resulting in regulatory action or data loss.**
- (vi) **If PI is moving from EU to US, Company has registered for Data Shield status (or registration is pending).**

Our privacy lawyers are happy to assist you in your review of your own or a potential target’s data practices and privacy policies in all stages of a merger or acquisition.

If you would like additional information, please contact any of the following FisherBroyles partners:

Atlanta

Carl Johnston
(404) 330-8179
carl.johnston@fisherbroyles.com

Boston

Peter Cahill
(617) 475-0094
peter.cahill@fisherbroyles.com

Chicago

Marty Robins
(847) 277-2580
martin.robins@fisherbroyles.com

Los Angeles

Steven Papkin
(310) 415-6254
steven.papkin@fisherbroyles.com

Palo Alto

Kimberly Booher
(650) 636-5958
Kimberly.booher@fisherbroyles.com

FisherBroyles, LLP - Cloud-based. Not Virtual™

Founded in 2002, FisherBroyles, LLP was the first in the U.S., and now the largest full-service, cloud-based law firm in the world. The Next Generation Law Firm has grown to approximately 150 attorneys in 20 offices nationwide. The FisherBroyles’ Law Firm 2.0[®] model leverages technology to offer a cost effective solution without sacrificing Big Law quality by eliminating overhead that does not add value to clients. Visit our website at www.fisherbroyles.com to learn more about our firm’s unique approach and how we can best meet your needs.

These materials have been prepared for informational purposes only, are not legal advice, and under rules applicable to the professional conduct of attorneys in various jurisdictions may be considered advertising materials. This information is not intended to create an attorney-client or similar relationship. Whether you need legal services and which lawyer you select are important decisions that should not be based on these materials alone.

© 2016 FisherBroyles LLP