KILPATRICK TOWNSEND

5 KEY TAKEAWAYS

RCG Webinar Series: Biometric Privacy Law in the US: Compliance Strategies and Litigation Trends

On January 21, 2020, Kilpatrick Townsend attorneys Vita Zeltser and John Brigagliano presented a webinar on U.S. biometric data privacy, as a part of Kilpatrick's regular Retail and Consumer Goods webinar series. The presenters offered strategies for in-house counsel to identify and mitigate legal risk associated with deploying technologies that collect or store biometrics.

The takeaways from the panel discussion include:

1

Legal counsel must determine whether their clients and their clients' vendors collect biometrics, and what legal regimes apply to that collection: To facilitate that inquiry and ensure that personnel across an organization can identify biometric information use, legal departments should inform key business stakeholders as to how biometrics are defined under applicable laws.

Of all of the U.S. laws governing biometrics, the Illinois Biometric Information Privacy Act ("BIPA") is the big one—and requires technical compliance: BIPA requires organizations to, among other requirements, execute a written release with the subject of the biometrics—merely providing a one way notice is insufficient. BIPA provides statutory damages of $5,000 for each intentional statutory violation of both substantive and technical requirements of the law, and has been the basis for an exploding number of class actions.

2

3

Retailers (and other companies whose premises are open to the public) may have to disable in-store surveillance features that collect visitors' biometrics in Illinios, and possibly in other jurisdictions: BIPA compliance is not practical for many surveillance use cases because the lack of privity of contract with the subjects of the biometrics collected makes executing a written release with those subjects impractical.

Vendors and customers can shift some compliance risks through contract, but the practical effect of contractual protection is limited: Customers can ensure, through contract, that vendors do not collect biometrics except as directed by the customer, and reinforce that restriction with an indemnification obligation. However, the practical usefulness of a vendor's indemnity may be limited, given the recent trend of multiple multi-million dollar BIPA class action lawsuits filed simultaneously against a vendor and many of its major customers, thus greatly straining the vendor's available resources. This concern would be especially pronounced in cases involving small vendors.

4

5

Issues relating to compliance with biometrics laws should be a regular part of a purchaser's M&A due diligence review process: Would-be purchasers in M&A transactions must determine whether target companies collect biometrics and, if so, whether the target's use of biometrics may feasibly comply with applicable law.

For more information, please contact:
Vita Zeltser, vzeltser@kilpatricktownsend.com
John Brigagliano, jbrigagliano@kilpartricktownsend.com

www.kilpatricktownsend.com