

Claimed Failure to Disclose GDPR's Collateral Impact Leads to Class Action Against Nielsen Holdings

In what could be a harbinger of things to come for business models negatively impacted by the throttling of data flow under the European Union's General Data Protection Regulation ("GDPR"), Nielsen Holdings ("Nielsen") was named in a putative class action complaint on August 22, 2018, for allegedly misrepresenting the anticipated effects of GDPR on Nielsen's business model. Importantly, the class action takes aim not at Nielsen's ability to comply with GDPR, but rather the effects of GDPR on the big data platforms used by Nielsen. Nielsen provides consumer market analytics, particularly regarding digital media and e-commerce. When big data platforms and associated analytic providers began restricting access to consumer data in order to comply with GDPR, it apparently negatively impacted Nielsen's business model. Those effects surfaced in Nielsen's latest Q2 financial report, causing its stock to drop by more than 25 percent, and giving rise to the class action claims.

The claims are based on Nielsen's downplaying of anticipated changes in the privacy space, as initially provided by the company's CEO, who stated, "For measurement, we still have the access to all the data that we need for our measurement products including our relationship with Facebook." When Nielsen released its Q2 report, however, the company conceded, "Our results are significantly below our expectations as revenues were impacted by GDPR and changes to the consumer data privacy landscape. We have several hundred clients and data partners in this space and market changes have been disruptive." In the Q2 report itself, Nielsen acknowledged it had missed its targets, and downgraded its EBITDA margin growth, net income, and free cash flow.

The claims are hardly a slam dunk. Beyond the traditional challenge of linking the difference in anticipated versus actual performance to a specific event like the ripple effects of GDPR, the plaintiff class will have to prove that Nielsen and its CEO knew—at the time it issued its public statements—that Nielsen likely would in fact be materially and negatively impacted by the GDPR's effect on the big data ecosystem, particularly the availability of data necessary for Nielsen's model. Critical to this inquiry will be the actual analysis conducted by or on behalf of Nielsen as to the impacts of GDPR on Facebook

Related Capabilities

- Privacy & Social Media
- Government Enforcement & Corporate Investigations
- Securities & Financial Services Litigation & Enforcement
- Class Action Litigation

and others, and on which Nielsen and its CEO may have relied in earlier statements designed to reassure investors.

The important take-away from these claims, certainly for publicly traded analytical services companies likely to be affected by changes in the privacy space but perhaps even others as well, will be to consider carefully any public statements about the impacts of GDPR and similar privacy initiatives in the US and abroad. Establishing that Nielsen knew its data sources were restricting access in a manner that would affect Nielsen's business model, and that Nielsen failed to reflect that knowledge in its public statements will be required to prove claims for violations of Sections 10(b) and 20(b) of the Exchange Act (the latter against Nielsen's individually named CEO and CFO), as well as Rule 10b-5 violations.

Many companies, including those squarely in the wheelhouse of new privacy requirements, rolled out new privacy policies and practices only moments before GDPR took effect, or are still in the process of doing so. Analysts are asking more informed and challenging questions about the impact of GDPR. While 'I honestly don't know' may be an accurate response and avoid liability for wrongly predicting the financial fallout from GDPR and similar initiatives, it may not be much comfort to investors.