Published on *The National Law Review* https://natlawreview.com

In with the New, Part III: 2014 Privacy, Advertising and Digital Media Predictions

Article By:

David Quinn Gacioch

Class Action Litigation Predictions

2014 is already shaping up to be an explosive year for privacy- and **data-security-related class actions**. Last December's data breach at Target has already led to more than 70 putative class actions being filed against the retailer. With recently disclosed data breaches at Neiman Marcus and Michaels Stores—and possibly more to come at other major retailers—court dockets will be flooded with these suits this year. And consumers are not the only ones filing class actions; banks that have incurred extra costs as a result of the data breaches are headed to court as well, with at least two putative class actions on behalf of banks filed so far against Target.

That volume of litigation related to the Target data breaches likely will be matched by a steady stream of class actions filed under the **TCPA.** 2013 was a busy year for the TCPA docket and I expect that the Federal Communications Commission's (FCC) stricter rules requiring express prior written consent from the called party, which took effect in October 2013, means that 2014 will be just as busy since the majority of TCPA class actions seek statutory damages for companies' failure to obtain consent before making autodialed or prerecorded voice calls or sending unsolicited text messages or faxes.

In 2014, I expect to see key decisions under the ECPA related to social media platforms and email providers capturing and using content from customers' emails and other messages for targeted advertising or other purposes. One district court has already denied a motion to dismiss an ECPA claim challenging this conduct and I predict that other decisions are forthcoming this year. Needless to say, decisions in favor of class-action plaintiffs in this area could have major implications for how social media sites and email providers do business.

Government Responses to Data Breaches

As significant data breaches continue to dominate the news, public awareness of data privacy and security issues will increase, as will their political appeal. I expect to see in 2014:

- Record numbers of breach reports to state and federal regulators, as awareness of reporting obligations spreads further and further across data owner, licensee, broker and transmitter

groups;

- More states committing more enforcement resources to data privacy and security, including budget dollars and dedicated attorney general's office units;
- More state/federal and multi-state coordination of investigations, leading to increased settlement leverage by enforcement authorities vis-à-vis firms under investigation; and
- Greater numbers and dollar values of settlements by the Federal Trade Commission (FTC) and state attorneys general than ever before.

Similarly, with the **HIPAA Omnibus Final Rule** going into effect on September 23, 2013, coupled with the late-2013 Department of Health and Human Services (HHS) Office of Inspector General Report decrying HHS **Office for Civil Rights' (OCR)** recent pace of HIPAA-related auditing and enforcement will lead to a jump in HIPAA breach reporting and harder lines taken by OCR with respect to investigation dispositions. Therefore, expect increased settlement counts and dollar values in the OCR enforcement during 2014, too.

Substantively, expect enforcement agencies to continue focusing their greatest attention on companies that they perceive as foot-dragging or stone-walling on notification obligations in the aftermath of breaches.

See Part I Here

See Part II Here

National Law Review, Volume IV, Number 32

Source URL:https://natlawreview.com/article/new-part-iii-2014-privacy-advertising-and-digital-media-predictions