

Cable Company Sued Over Data Retention and Privacy Practices

OCTOBER 25, 2012

A class action lawsuit was recently filed in California against Bright House Networks LLC, a cable operator, alleging that the company violated the [Cable Communications Policy Act](#) (47 U.S.C. § 551(a), (e)) by indefinitely retaining customers' personally identifiable information and failing to send annual privacy notices to customers. The Act requires that cable operators destroy the personally identifiable information of former subscribers if the information is no longer necessary for the purpose for which it was collected, and if there are no outstanding requests or orders for such information. The Act also requires cable operators to provide annual notice of (1) the nature of personally identifiable information collected, (2) the nature, frequency, and purpose of any disclosure of that information, (3) the period during which such information will be maintained, and (4) the times and place at which the subscriber may have access to such information. Plaintiffs allege that Bright House failed to meet both the notice and destruction requirements laid out in the statute. The complaint also quotes the Bright House privacy policy, which states that subscriber data is destroyed if it is no longer needed for business purposes, but in practice data is retained indefinitely. Plaintiffs further allege violations of California state statutes and common law claims, and have requested injunctive relief as well as liquidated, punitive, and compensatory damages.

Tip: While this case falls under a specific statute which may not apply to all, it serves as a reminder that class action lawyers are scrutinizing companies privacy practices closely. Those subject to the Act should ensure their practices comply, and those who do not fall under its ambit would nevertheless be well served to ensure that they are prepared in the event of a consumer complaint. Steps to prepare include making sure a privacy policy accurately reflects current corporate data security and privacy practices and addresses current areas of concern for consumers and regulators alike. These include how the information will be used, with whom it will be shared, and the choices consumers might have over that use.

These tips have been created for information and planning purposes. They are not intended to be, nor should they be substituted for, legal advice, which turns on specific facts.

2 Min Read

Related Topics

Communications Privacy

Data Breach

Related Capabilities

Privacy & Data Security

This entry has been created for information and planning purposes. It is not intended to be, nor should it be substituted for, legal advice, which turns on specific facts.