DAVIS GILBERT

Lawmakers React to New Technology Trends With Updates and Amendments

5th Edition: Trends in Marketing Communications Law

Federal and State Updates

In 2017, the Federal Trade Commission (FTC) continued to focus on data collection and information security practices, calling for more nuanced consent and disclosure practices and the implementation of adequate information security infrastructures and controls to protect consumer data. The FTC also emphasized compliance by domestic businesses under the new EU-U.S. Privacy Shield. There continues to be uncertainty regarding the FTC's direction and focus in 2018 as the new Commission and Chairman were only recently confirmed by the Senate on April 27, 2018.

Developments on the state level are also having a significant impact on the industry. Delaware made several amendments to its data breach notification law, including an expanded definition of a computer security breach and a new requirement that all entities operating within the state must safeguard personal information. The amendment also expanded the definition of "Personal Information" to include information such as passport number, a username or email address, in combination with a password or security question and answer that would permit access to an online account; certain medical or health information; unique biometric data used for authentication purposes; and an individual's taxpayer identification number. The new amendment also contains a 60-day notification period and mandatory identify theft prevention and mitigation services for a year for breaches involving a social security number. Meanwhile, the final states without such laws, South Dakota and Alabama, have very recently passed security breach notification bills.

GDPR and PECR

Companies are preparing for the European Union's new General Data Protection Regulation (GDPR) to ensure compliance by the enforcement commencement date of May 25, 2018. Compared to its predecessor, the EU Data Protection Directive (the Directive), the GDPR will impose more stringent consumer privacy requirements on companies handling personal data of EU citizens. As the deadline nears, companies subject to the GDPR should reevaluate their internal policies and practices, and conduct company-wide data audits to ensure compliance. Prior practices compliant with the Directive may no longer suffice, and violations can result in substantial fines. For example, consent that has been obtained prior to the GDPR's effective date that does not meet the new requirements will need to be re-examined and possibly require a re-opt-in prior to the upcoming deadline. In addition, companies should be mindful of their third-party service providers that also collect and process data (e.g., market research and analytics), and ensure applicable GDPR requirements are included in their vendor contracts.

While all eyes are on the GDPR, companies should not forget about the Regulation on Privacy and Electronic Communications (ePR or e-Privacy Regulation), which repeals the 2002 ePrivacy Directive, that is expected to go into effect after the GDPR. ePR covers the storing or accessing of information on a user's device (including, but not limited to, the use of cookies, email and texting). While ePR generally requires consent, the GDPR has a number of legal bases for the processing of personal data, including consent and legitimate interest. ePR's adoption is pending and the implementation date is still unclear.

Key Takeaways

- As companies develop and use Internet-connected technologies to reach consumers and collect data across multiple devices, greater regulatory oversight to protect consumers gains momentum in 2018.
- Companies should be actively preparing for the GDPR and become compliant before May 25, 2018, and assess whether updates to PECR will affect the way they use electronic communications and cookies.
- Companies should keep up-to-date on state laws pertaining to data security, privacy and breach notification.

Related People

Gary Kibel
Partner
212 468 4918
gkibel@dglaw.com

Oriyan Gitig
Counsel
212 468 4880
ogitig@dglaw.com