DAVIS GILBERT

Data Privacy and Security Laws Get Stronger, and Face New Challenges

4th Edition: Trends in Marketing Communications Law

As data becomes more and more commoditized, domestic and international laws and regulatory actions continue to focus on privacy rights and data security.

The Federal Trade Commission (FTC) has issued several reports, tools, and guidance in the privacy and data security area, including a report on balancing privacy and innovation, a tool to help health application developers better understand the federal laws that apply to their applications, and an online cross-device tracking report focused on new tracking technologies in apps and across multiple devices.

The FTC also has increased its enforcement efforts, with high profile cases involving companies including InMobi, Oracle, Vulcun, Ashley Madison and ASUS. Whether this enforcement trend will continue may depend, in part, on who the Trump administration will appoint to occupy the vacant FTC commissioner positions.

While the FTC continues to strengthen its privacy and data security standards, states have been updating their privacy regulations and protections. Many states impose a “reasonable safeguards” standard to protect personal information, but it has been unclear what constitutes “reasonable safeguards.”

Massachusetts and Oregon have set out more specifics in their interpretation of “reasonable safeguards,” but California was the first state to define it. In a recent data breach report, the California Attorney General opined that failure to implement all 20 controls listed in the Center for Internet Security’s Critical Security Controls constituted a lack of reasonable security.

A number of international privacy law developments also have implications for marketers and other businesses. The United States and the European Union approved the EU-U.S. Privacy Shield and the EU adopted the General Data Protection Regulation (GDPR), effectively replacing the EU Data Protection Directive and imposing new consumer privacy requirements on companies handling data from the EU with a compliance deadline of May 2018.

Artificial intelligence (AI) has joined “Big Data” and the “Internet of Things” as new privacy challenges. Companies such as Amazon, Google and Apple have rolled out AI-enhanced entertainment systems that depend on data collection (e.g., Amazon Echo, Google Home and Apple HomeKit). Consumers have shown that they are willing to give out their data in exchange for new “convenience technologies,” but like all new technologies, this involves risk, and the “machine learning” characteristic of AI technologies may pose challenges for a consent-based model of data collection. How this form of data collection will affect the regulatory landscape remains to be seen.

Key Takeaways

- Companies should reassess their data security infrastructure and written privacy and information security policies.

- Companies should assess whether they have in place the necessary controls that constitute “reasonable safeguards.”
- Companies that handle personal data of EU residents or process data in the EU need to ensure that they are in compliance with the GDPR before the May 2018 deadline.
- Companies involved in AI technology should put privacy at the forefront of their priorities.

Related People

Gary Kibel
Partner
212 468 4918
gkibel@dglaw.com

Oriyan Gitig
Counsel
212 468 4880
ogitig@dglaw.com