Israeli Consumer Protection and Fair Trade Authority issues draft guidance on disclosure obligations for IoT products

The Commissioner of the Consumer Protection and Fair Trade Authority (the "**Commissioner**"), together with the National Cyber Directorate, have recently published a draft guidance with respect to disclosures that must be made to consumers purchasing IoT products (the "**Draft Guidance**").

The Draft Guidance mentions that while IoT products can be very useful and efficient, the use of such products entails cyber and information security risks, such as data leaks, damage to the product, and even personal injury. According to the Draft Guidance, the National Cyber Directorate has identified numerous cases in which IoT products used by consumers and organizations were hacked, such as home cameras, "smart home" systems, smart TVs, baby monitors, etc.

The Israeli Consumer Protection Law, 1981 (the "**Consumer Law**"), includes a prohibition on deception, and prohibits any act or omission that may deceive a consumer on any substantial matter relating to a transaction, including the uses for which the product may be utilized, the benefit that can be derived from the product and the risks involved in the use of the product. Additionally, the Consumer Law imposes disclosure obligations, such as disclosure regarding features in the product that require handling the product in a certain manner to avoid damage to the product or personal injury.

In that context, the Draft Guidance imposes an obligation to disclose to consumers that IoT products may be misused by hackers for carrying out cyber-attacks. Such disclosure should stress the importance of changing the product's default password and should explain how to do so. The disclosure should mention whether the manufacturer of the product intends to issue security updates for the product, the timeframe for the issuance of such updates, and an explanation regarding the installation of such security updates. To the extent that the product does not include an option for changing the default password or does not include security updates, such product would be considered flawed or of low quality, and such information would also need to be disclosed.

The aforementioned disclosure should be made **prior to** the consumer purchasing an IoT product and during **all stages of the transaction**, including advertising and marketing. The disclosure must be prominent, clear and understandable to the consumer, whether the disclosure is given in a publication, in writing or orally.

Additionally, the Draft Guidance includes several steps which the National Cyber Directorate advises to take in order to limit the aforementioned risks in home cameras, such as changing the product's default password, installing software updates issued by the manufacturer, implementing two-factor authentication (to the extent available), reviewing of the product's settings, etc.

The Draft Guidance marks an important development as it paves the road for imposing cyber-security and data protection requirements through the Consumer Law. Violation of such requirements may expose businesses, among others, to administrative fines and class actions.

Please feel free to contact us with any questions that you have on this matter.

Assaf Harel, Partner
assafh@gornitzky.com

Rebecca Genis, Senior Associate
rebeccage@gornitzky.com