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

Internet Peeping Toms and The Internet of Things Face New Hurdles: Federal Trade Commission (FTC) Settles with TRENDnet, Inc.

Article By:

Privacy & Security Practice Group at Mintz Levin

The **Federal Trade Commission** ("**FTC**") recently entered into a settlement agreement with TRENDnet, Inc., a company that sells Internet Protocol ("IP") cameras that allow customers to monitor their homes remotely over the Internet. Notably, this is the FTC's first action against a seller of everyday products that connect to the Internet and other mobile devices, commonly referred to as the "Internet of Things."

The Complaint

In its complaint, the FTC alleged that, despite representing to its customers that TRENDnet's IP cameras are "secure," TRENDnet failed to reasonably secure its IP cameras against unauthorized access by third parties. According to the FTC, TRENDnet transmitted user login credentials in clear, readable text over the Internet and stored user credentials on a user's mobile device in clear, readable text, despite the availability of free software to secure the transmissions and the stored credentials. The FTC Further alleged that TRENDnet failed to employ reasonable and appropriate security in the design and testing of the software that it provided consumers for its IP cameras.

Due to TRENDnet's inadequate security measures, in January 2012, a hacker exploited the vulnerabilities of the TRENDnet system and posted live feeds for nearly 700 of TRENDnet's IP cameras, including customers that had not made their video feeds public. These video feeds displayed people in their homes, including sleeping babies and young children playing. Once TRENDnet learned of this flaw, it uploaded a software patch and attempted to alert its customers of the need to update their IP cameras through TRENDnet's website.

The Settlement

Last week, TRENDnet entered into a settlement agreement with the FTC to resolve the FTC's claims. Pursuant to the settlement agreement, TRENDnet has agreed that it will not misrepresent:

- the extent to which its products or services maintain and protect the security of its IP cameras;

- the security, privacy, confidentiality or integrity of the information that its IP cameras or other devices transmit; or

- the extent to which a consumer can control the security of the information transmitted by the IP cameras.

What's more, TRENDnet is required to establish, implement and maintain a comprehensive security program that is reasonably designed to address security risks that could result in unauthorized access to the IP cameras or other devices, and to protect the security, confidentiality and integrity of the information that its IP cameras or other devices transmit. TRENDnet is further required to conduct initial and biennial assessment and reports of such security program by an independent third-party professional every two years for the next twenty years. Again, some real bottom line costs as a result of these settlements.

Finally, in addition to the measures that TRENDnet must take to protect its customers in the future, TRENDnet must also notify all of its current customers about the flaw in the IP cameras that allowed third parties to access the live feed of TRENDnet customers, and TRENDnet must provide these customers with instructions on how to remove this flaw.

The TRENDnet settlement is the FTC's first step at regulating data security in the land of the Internet of Things. Keep a look out to see whether this becomes the FTC's next hot topic.

National Law Review, Volume III, Number 255