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

Federal Trade Commission (FTC) and the "Internet of Things": Franchisor on the Hook

Article By:

Privacy & Security Practice Group at Mintz Levin

Last fall the **Federal Trade Commission** brought cases against a software developer and rent-to-own stores that secretly monitored people in their homes. The developer provided the stores with software that had a "Detective Mode" that once enabled allowed the stores to log key strokes, capture screen shots, take pictures using the computer's webcam, track the location of the computers and it was also able to launch a fake software program registration to collect consumer information. The stores put it on computers and rented them to users without the user's knowledge that the software would be monitoring them. The stores remotely activated the software and caught unsuspecting consumers doing everything from making breakfast to making whoopee. It is alleged that the software also grabbed the users' login credentials for financial sites, social media and other sites accessed by the user.

The case took another turn this week as the FTC proposed a settlement with the franchisor, Aaron's. Why was the franchisor brought into the mix? Because, according to the complaint, Aaron's provided their franchisees with "the technical capacity to access and use" the software.

In order to use the technology and activate Detective Mode the franchisees needed to access the software website and provide an email address where the captured information would be sent. The franchisees used corporate email accounts provided by Aaron's and the emails were routed through Aaron's corporate headquarters and stored on servers owned, controlled and maintained by Aaron's.

But that's not all: The franchisees experienced glitches when trying to install the software due to Aaron's network security features and some franchisees had to seek written permission from Aaron's to access the software website. Aaron's senior management approved these requests. Aaron's also helped the franchisees install the software on computers by publishing step-by-step instructions that told franchisees how to handle any technical difficulties they encountered when trying to install the software.

The information snatched by the software was sent to Aaron's email accounts and Aaron's network had over 100,000 Detective Mode messages from those rented computers. Perhaps you're thinking, "well maybe Aaron's didn't know what type of information was being swiped from the computers and stored on their servers?" Although that would make sense, you would be wrong. An IT

employee who reviewed Detective Mode images described the program as “very intrusive” in an email to Aaron’s chief information officer. Aaron’s also put Detective Mode on a franchisee meeting agenda and considered adding it to computers rented at Aaron’s corporate-owned stores.

When Aaron’s received complaints from customers it didn’t shut down the web portal and stop franchisees from accessing the software website immediately — it took them 6 months.

The 20-year consent order bars Aaron’s from benefitting from the information it collected via the software and requires them to destroy all improperly collected data. The order also requires Aaron’s to conduct annual monitoring and oversight of its franchisees to ensure they are meeting the requirements that apply to Aaron’s and its corporate stores. Franchisees that don’t meet those requirements should be cut loose.

The FTC blog post on this case reminds us that the FTC Act is broad. In this case the FTC brought suit against the software developer (including corporate officers), retailers that used the software and Aaron’s.

National Law Review, Volume III, Number 296