wiley

NEWSLETTER

FTC Holds Franchisor Liable for Franchisees' Breach of Consumer Privacy

December 3, 2013

For the past decade, the Federal Trade Commission (FTC) has engaged in various enforcement actions, primarily using its jurisdiction over deceptive and unfair trade practices, to address various privacy and security failings by companies across the country. Many of these cases have reflected a failure to provide appropriate safeguards for consumer or employee information, starting with the BJ's Wholesale case in 2005 (available at www.ftc.gov/opa/2005/06/bjswholesale.shtm). The FTC's authority for this line of cases currently is under attack by the Wyndham Hotel Group, which faces an FTC enforcement action initiated in 2012 following a security breach involving its hotel reservation system. Wyndham's motion to dismiss was argued on November 7 before the U.S. District Court in New Jersey. While the FTC awaits the fate of its privacy and security enforcement authority in connection with the Wyndham litigation, it is continuing to move forward in making new law with the goal of preventing consumer harm and protecting consumers from inappropriate activity.

While many of the FTC's recent cases have focused on ineffective security practices related to consumer information, the most recent case—involving Aaron's, Inc., a "rent-to-own retailer" based in Atlanta—focuses on privacy-related activity and may well be the first case to address the franchisor's liability for franchisee conduct that impacts consumer privacy. The case is also important because (1) it concerns specific activity that the FTC deems inappropriate for the collection and use of consumer information, and (2) it imposes a standard on franchisors related (for the most part) to inappropriate activities by their franchisees.

In the Aaron's case, the focus is more generally on "deceptive" behavior. While there are some security-related components to the case (primarily involving potential security threats to consumers from illicit gathering of information), the primary allegations against Aaron's arise from deceptive practices used in gathering information about individual consumers renting computers from Aaron's franchised stores. The FTC concluded that those methods created a significant risk of harm to these consumers.

The gist of the case is straightforward. One of the products rented by Aaron's (through both company-owned and franchised stores) is computer equipment. Various Aaron's franchisees—not the company-owned stores—installed computer-monitoring software known as PC Rental Agent in computers available for rent to consumers. According to the FTC press release, the software "surreptitiously tracked consumers' locations, captured images through the computers' webcams—including those of adults engaged in intimate activities—

and activated key loggers that captured users' login credentials for email accounts and financial and social media sites." The software also provided an opportunity to take webcam pictures of consumers in their homes, all without the knowledge of the consumer. In addition, the software allowed the franchisees to disable a computer remotely. (Note: In an earlier case that attracted less attention, the FTC had pursued separate enforcement actions against the software design firm and various franchisees in their capacity as franchisees. See "FTC Halts Computer Spying," *Privacy In Focus* (October 2012). According to the complaint, "Aaron's franchisees used this illicitly gathered data to assist in collecting past-due payments and recovering computers after default."

The Case Against the Franchisor

The FTC found that Aaron's—by "enabling their franchisees to use this invasive software"—was itself in violation of the consumer's rights, and had violated the FTC rules against deceptive practices, even though this software was not used in any of the company-owned stores.

While Aaron's did not use this technology in its company-owned stores, the FTC determined that Aaron's "knowingly assisted its franchisees" in implementing and using this software.

Specifically:

- Aaron's allowed its franchisees to access the software designer's website, which was necessary in order for them to use PC Rental Agent (and, according to the FTC, without this permission, many of the franchisees could not have activated this software);
- Aaron's corporate server was used to transmit and store emails containing content obtained through the monitoring. Aaron's provided email accounts to its franchisees that many of them used to receive messages sent from the software firm containing information captured by the software from consumers; and
- Aaron's provided franchisees with vital technical support for the software program, such as publishing troubleshooting advice about installing the program on rented computers and avoiding conflicts with antivirus software.

To the FTC, these activities were sufficient to take action against Aaron's for its own role in these practices, as having "facilitated a violation of many consumers' privacy."

The Consumer Harm

In contrast to many of its information security cases, the FTC found that there was identifiable and actual harm to consumers in this situation. (Many of the safeguards cases involved risks to personal information, rather than identifiable harm). Here, according to the FTC, "consumers were substantially harmed." The FTC also asserted that Aaron's "knew" that the data that was being gathered through the software "could be highly intrusive and invaded consumers' privacy." Through Aaron's "knowing support" of the franchisees that used this software, Aaron's (1) placed consumers at risk of exposure of their personal, financial account access, and

medical information; (2) injured consumers through the "unwarranted invasion into the peaceful enjoyment of their homes;" and (3) caused actual harm through the "surreptitious capture of the private details of individual and family life—including images of visitors, children, family interactions, partially undressed individuals, and people engaged in intimate conduct." In addition, because this software operated without any consumer consent, in secret, and consumers could not remove the software, "consumers were unable to reasonably avoid this harm, which was neither trivial nor speculative." The FTC also found that there "were no countervailing benefits to consumers or to Aaron's that outweighed this harm."

The Resolution

The consent order resolving the FTC's administrative complaint contains a wide variety of prohibitions on Aaron's going forward (that in practice will be coupled with sanctions imposed on the individual franchisees in the earlier action). The consent order is broken down into particular sections, each focused on an element of the harm or inappropriate activity. According to the "Analysis of Proposed Consent Order to Aid Public Comment," these prohibitions are:

- Section I of the order prohibits Aaron's from using monitoring technology on computers and from receiving, storing, or communicating information about consumers collected with such technology.
- Section II prohibits Aaron's use of geophysical location-tracking technology on any consumer product without notifying and obtaining consent from renters. Aaron's must also notify a user of a rented computer immediately prior to activating tracking technology on that device, unless Aaron's has a reasonable basis to believe that the computer has been stolen and a police report has been filed.
- Both Sections I and II also contain provisos that permit Aaron's to use monitoring or geophysical location-tracking technology for purposes of providing requested customer assistance, where the consumer has consented to the use of the technology and any information collected is used only to provide the requested assistance.
- Section III of the proposed order prohibits the deceptive gathering of consumer information, which will bar Aaron's from using fake software registration notices or similar deceptive tactics.
- Section IV will prevent Aaron's from using any consumer information to collect on rental contracts that was improperly obtained through monitoring technology, tracking technology, or deceptive notices that appear on computer screens.
- Section V requires the destruction of any data gathered using monitoring or tracking technology without the requisite notice and consent or obtained under false pretenses, and mandates the encryption of any properly collected data when it is transmitted.
- Section VI prohibits Aaron's from making any misrepresentations about the privacy or security of consumer information it collects.

The Implications

As with many (but clearly not all) of the FTC's cases, the particular practices at issue seem highly inappropriate even if the FTC's authority is disputed. These kinds of practices—where there is aggressive, broad, and hidden monitoring of clearly identifiable individual details that is well beyond the reasonable expectations of any consumer—will virtually never be perceived by a regulator as appropriate without a specific and really good reason. Outside of a specific regulatory framework, these practices simply do not pass the sniff test—they are wildly out of line with reasonable activity. This "good sense" reality check should be a component of any company's decisions related to the collection of consumer information. In fact, given the inherent unreasonableness of these activities, this is exactly the type of scenario where a privacy officer should provide an appropriate check on the inappropriate activity—if the privacy officer is qualified and consulted before the activity takes place. (The FTC documents do not discuss any role played by an Aaron's privacy officer.) In addition, this highlights the need for privacy officers in a wider range of businesses, even those that are not directly regulated by specific privacy laws. While the limits of the FTC's authority to deem particular practices unfair or deceptive are not at all clear, this is an example where the better judgment—in a system where personal privacy is increasingly regulated—is to simply "not do that," without the need for any more detailed explanation.

For franchisors, the issue is more complicated and worthy of ongoing evaluation. Here, Aaron's—the franchisor—is deemed to have been an active participant in the franchisees' activities through its knowledge of the practice and its technical support for the software monitoring, even though the company did not initiate tracking of specific renters or utilize the software in company stores. Accordingly, the case—on its own—stands for little more than the principle that a franchisor can be held responsible for the primary acts of a franchisee where the franchisor assists those acts in a meaningful way.

The broader issue—and one that is raised but not resolved by this case—involves a franchisor's obligation to monitor the activities of franchisees in connection with the use and disclosure of consumer information. How much "involvement" or "knowledge" would have been enough for the FTC to act in this case? Would "knowledge" without involvement have sufficed? Would use of the corporate email system alone have been sufficient? Clearly, there is an ongoing and direct tension between the efforts of franchisors to maintain an appropriate legal separation from franchisees and the involvement of the franchisor in the activities of the franchisees. Some of these activities are primarily reputational—where a franchisee has a security breach, the headlines are likely to involve the franchisor even if direct legal responsibility under the breach notification regulations rests with the franchisee. (Obviously, a class of plaintiffs may bring a claim against the franchisor as well, and the actions of a franchisee may invite an investigation from appropriate regulators).

Accordingly, franchisors may wish to review their policies related to privacy and security instructions and principles for franchisees, including determination of whether any ongoing monitoring and auditing will be thought unfair. Moreover, a franchisor should use a privacy officer—or someone with similar skills—to evaluate and analyze any information gathering activities of both the franchisor and the franchisees, to put these activities in an appropriate context and assess the risks to consumers and the company potentially arising from these activities.