Fox Rothschild Podcast

Featuring Litigation Partner John Gotaskie in Pittsburgh

We are talking today about franchising and its privacy implications with John Gotaskie on Fox Rothschild Podcast. John is a partner and litigator with Fox Rothschild in Pittsburgh. He represents clients in diverse legal matters, including franchising and complex commercial litigation as well as creditor's rights and social media matters. John, good morning.

John Gotaskie: Good morning. Thank you.

***Question**: John, you recently wrote an interesting piece for Fox Rothschild's* Franchise Law Update Blog*. The post was entitled "Do You Have a Plan for Deploying Monitoring and Tracking Software?" – and you wrote an attention-getting subtitle.*

John Gotaskie: Yes, my point was that if an organization or franchise organization doesn't have a plan for deploying and monitoring tracking software, the Federal Trade Commission may want to speak with them.

***Question**: John, are there risks for organizations that use software to monitor and track user data?*

John Gotaskie: Indeed there are. Organizations that use tracking software need to proactively think about the appropriate use of monitoring and tracking software before they're deploying it, and tailor its use to legitimate needs that are disclosed to the public.

***Question**: John, can you provide our listeners with a good example?*

John Gotaskie: Well, a recent FTC action against Aaron's, a national Rent-to-Own retail store with approximately 1300 corporate locations and 700 franchised locations, provides us with a good example. Specifically, the FTC had filed a complaint against Aaron's for violation of a section of the FTC Act.

The FTC's complaint challenged Aaron's use of privacy-invasive software installed on computers rented to its customers. Aaron's installed the software on computers rented at company stores, and according to the FTC, "knowingly assisted" and encouraged its franchisees to utilize the software.

***Question**: John, from a technical standpoint, how does software potentially invade someone's privacy?*

John Gotaskie: This case provides a good example. The software that Aaron's was using had two modes. In the first mode, the software surreptitiously captured private, confidential and personal information about its customers. Aaron's and its franchisees then used this information to assist in collecting past-due accounts and recovering computers after default.

Now in the second mode, which was called "Detective Mode," the software could log keystrokes, capture screen shots and activate a computer's webcam, all without the user knowing. According to the FTC, this detective mode even collected sensitive information through the use of fake software registration notices. You know how they'll pop up on your screen and you have to accept them to keep using? This was another way that the program worked. Yet another feature of the Detective Mode allowed stores to track the physical location of rented computers using Wi-Fi hotspot information. Interestingly, the FTC's complaint stated that at least one franchisee was rather "uncomfortable with the ability to see the customer through the webcam." The webcams were allegedly used in fact to capture images of not just customers using their computers but their families, children and even guests in their homes.

***Question**: John, how was this information ultimately used?*

John Gotaskie: This is interesting because all of the information collected by the software was ultimately routed to the stores — including stores owned and operated by franchisees — through Aaron's corporate computers. In other words, the laptop computer that was rented would collect this information using the program. It would be sent to Aaron's corporate offices, and then distributed back out to the stores from where the computer had been rented. Aaron's was well aware of the large volume of sensitive information being collected because its own IT professionals noted the large volume of information and found the information reported to be intrusive. In fact, at one point the company was even sued, along with a franchisee, by a customer for state and federal privacy violations. Nonetheless, despite that suit, the program did not formally end until the end of 2011, and Aaron's in fact received the last batch of information collected by the program in 2012.

***Question**: John, did this collection of data cause actual consumer harm?*

John Gotaskie: The FTC certainly thought so. The consent order prohibits Aaron's from using monitoring technology on computers and from receiving, storing or communicating information collected from customers. It further prevents the use of geophysical location tracking software without notifying and obtaining prior consent from customers for its use. Even then, Aaron's must notify a user before activating the tracking software unless it has a reasonable basis to believe a computer has been stolen and a police report filed.

Similarly, Aaron's may use the monitoring or geo-tracking software for purposes of providing customer support, but again only where the customer has affirmatively consented to its use. Finally, all information already collected, while it already can't be distributed, must also be destroyed. And a compliance report must have been filed within 60 days of the order, and the order will remain in place for a total of 20 years.

***Question**: John, what are the effects of the FTC action and consent decree on the franchisees of Aaron's?*

John Gotaskie: That's a good question, because it turns out that the provisions of the consent order make it explicitly applicable to all of Aaron's franchisees, and require Aaron's to oversee and monitor its own franchisees' compliance with the "core constraints" imposed by the consent order. Don't track; get the permission ahead of time; things like that. Aaron's must monitor its franchisees' compliance with all of those constraints on at least an annual basis, which of course is going to increase the compliance costs for the company as well as every franchisee. If it discovers any violation, Aaron's has to take immediate action to correct the franchisee's practices. And, if the franchisee does not change its practices, Aaron's is required under the order to terminate that franchisee.

***Question**: John, it sounds like the FTC action and consent decree could be quite costly.*

John Gotaskie: It will be. They'll be costly not only for Aaron's but also for its franchisees. Moreover, as I've posted before on the blog, the consent decree demonstrates that the FTC is and will continue to be hyper-vigilant regarding these computer and data privacy issues even in the absence of new mandates from a divided Congress.

***Question**: John, what do you see as the takeaway lessons from this example?*

John Gotaskie: The basic thing is to think ahead and plan a little bit before you start deploying this monitoring and tracking software. There's a couple steps you should really think about. One, when it comes to data collection, use some common sense. The franchisee who felt uncomfortable and reported back his concerns about viewing his customers on the webcam, well he was clearly onto something. If it doesn't seem right, doesn't feel right, you probably shouldn't be doing it.

Next, disclose the existence of the tracking software to your customers. The FTC in this case was particularly bothered by the fact that even the existence of the software was hidden and concealed from its customers.

And then last, be explicit about what you are collecting, and make sure it fits your legitimate business goals. The FTC recognized here that stolen computers and computer operational assistance were legitimate and appropriate uses of the software if it had been disclosed to the customers. Moreover, I would add that while not an issue in this case, I would expect little difficulty with explicit advance notice to a consumer that a rented computer could be geo-tracked and/or shut down remotely if payments weren't made on time.

***Narrator**: Well, thank you John. Listeners, to confidentially discuss whether monitoring and tracking software impact your business, please contact John at 412-394-5528 or jgotaskie – that's J-G-O-T-A-S-K-I-E – at foxrothschild.com.*

Fox Rothschild LLP is a full service law firm built to serve business leaders, backed by 550 lawyers coast to coast. Our clients come to us because we understand their issues, their priorities and the way they think. We help clients manage risk and make better decisions by offering practical advice. Visit us on the web at www.foxrothschild.com.

# # # #