

Cybersecurity Group Of The Year: Shook Hardy

By James Boyle

Law360 (February 2, 2022, 2:02 PM EST) -- Shook Hardy & Bacon LLP last year got a burgeoning class action case accusing the Whirlpool Corp. of using software to illegally track users' behaviors on its website tossed, earning the firm a spot among Law360's 2021 Cybersecurity & Privacy Groups of the Year.

The firm's cybersecurity and privacy practice has about 30 attorneys located throughout its 17 offices, with the bulk of its leadership concentrated in Miami and Chicago.

"We have a very fluid group," said practice chair Alfred Saikali. "If there is a data breach lawsuit filed in Florida, we have people from our Denver and San Francisco offices working on it."

Practice members specialize in three particular areas of cybersecurity and data privacy, Saikali told Law360: state and federal data privacy compliance, privacy litigation matters, and biometric privacy issues.

Emerging technology trends have made cybersecurity and data privacy one of the hottest areas for Shook Hardy, Saikali said. In-house attorneys for many of the firm's corporate clients have the most inquiries for his team, asking what companies are allowed to do with their customers' personal information.

"Companies are using data analytics more and more about the customers," Saikali said. "Then you get into the secondary market and the possibility of selling information to third parties. There are all these rules that clients want to know about."

The recent rise of ransomware attacks has also been a point of concern for Shook Hardy's clients, Saikali said. His team has assisted on more than a hundred ransomware attacks in recent years, he said, and he has seen companies crippled by not taking the right proactive steps.

Shook Hardy's cybersecurity and data privacy team has also fulfilled one of its top priorities by becoming a leading authority on biometric privacy laws. Melissa Siebert leads that effort from the firm's Chicago office, located in the state with one of the toughest biometric laws in the country: Illinois' Biometric Information Privacy Act. She said her BIPA team is popular for some of the firm's associates hungry for appellate court experience.



"It is not unusual for us to have significant engagement in multiple state and federal courts every month," Siebert said. "We had fairly recent associates, not even in their third year, writing briefs for an appeal in the Seventh Circuit. It's a great training ground and a great opportunity for young lawyers."

A lot of the cybersecurity and data privacy practice group's focus is on keeping clients from becoming overwhelmed by aggressive plaintiffs' attorneys looking to exploit privacy laws for class action cases.

Such was the situation Whirlpool faced when attorneys used a federal wiretap communications law to accuse it of recording the private actions of website visitors when it used session replay technology to track activity on its website. The software shows how visitors interact with the site and tells the company which products are clicked on and which users are putting items in the shopping cart but not checking out, Saikali said.

A successful class action could have found the company facing a fine of \$1,000 per person, multiplied by millions of visitors to the site. This prospect put "the fear of God in a lot of companies," Saikali said.

Fortunately, he said, the judge in the U.S. District Court for the Southern District of Florida agreed with Shook Hardy's argument that Whirlpool never contemplated whether its technology violated wiretap laws, and none of the information was intercepted. The use of the software was disclosed by a privacy notice on the site. The complaints were dismissed with prejudice in July.

"The plaintiffs' bar is trying to be novel by taking existing laws and applying new technologies," Saikali said. "Sometimes they win and hit big, and sometimes they fail. Shook Hardy got a quick win and set the standard early on this issue for other judges to dismiss."

Shook Hardy's BIPA team has also been on the forefront of setting the standards that creates a balance between an employee who wants to protect their privacy and a company's need to have certain information to serve the employee. Several decisions and appeals on the use of biometric technology have centered on timekeeping software.

"Illinois employers are getting sued by a law that was never intended to be an employment law," Siebert said. "This is not on the poster in the lunchroom. All the employers are doing is using technology to make the workplace more efficient and time recording more accurate to comply with other laws."

Companies and organizations, including hospitals and the Salvation Army, use finger scans for employees to clock in and out of work, and they are then sued under a little known law that doesn't make sense in the use of the technology, Siebert said.

"The lawsuits don't take into account the reality of the situation, that people are clocking in and out to get paid," she said. "It is not a privacy breach. Is this really the intent of the BIPA statute, to create 2,500 lawsuits by folks who voluntarily use the technology?"



Alfred Saikali



Melissa Siebert