FTC Will Stay Privacy, Security Course, Departing Rich Says

By Jimmy H. Koo

The FTC should continue its privacy and data security enforcement efforts, support international data transfer mechanisms and continue to grow its technology oversight capabilities, departing Director of Bureau of Consumer Protection Jessica Rich told Bloomberg BNA in a sit-down exit interview.

The Federal Trade Commission must keep pace with rapidly-evolving technologies if it is to continue succeeding in its role as the leading U.S. consumer privacy agency, Rich said.

The proliferation of the internet of things (IoT) has fundamentally changed the notion of privacy and security, and consumers need better tools to make informed choices over how their data is handled, she said. Ultimately, privacy policy must be driven by market forces, Rich said.

Rich held a variety of positions at the FTC since she came on board in 1991, including deputy director, associate director of the Division of Financial Practices, and acting associate director and assistant director of the Division of Privacy and Identity Protection. She was appointed director of Bureau of Consumer Protection (BCP) in June 2013.

President Donald Trump named Washington lawyer and FTC veteran Thomas B. Pahl to take the helm as acting director of the BCP following Rich's departure Feb. 17.

Regardless of the change, the FTC will likely continue its privacy and data security enforcement efforts, support international data transfer mechanisms and continue to grow its technology oversight capabilities, Rich said.

Focus on Evolving Technologies

Under her leadership, the FTC expanded its privacy program, going from some four to nearly 50 attorneys dedicated to privacy and security issues, Rich said.

Rich led the commission's efforts to expand its technological expertise and took a leadership role in developing the first enforcement cases involving the internet and the application of the FTC Act to address privacy and security issues, she told Bloomberg BNA.

Rich said she ensured that commission staff had the tools to understand new technologies and make sure companies are complying with basic consumer protection principles. She also made structural changes in the FTC by starting the Mobile Tech Unit, which eventually became the Office of Technology Research and Investigation. Rich also developed foundational rules, including the Children's Online Privacy Protection Rule.

Issues related to privacy and security are much more complex and the traditional notion of notice and consent—a “one-to-one understanding of ‘tell me what you're collecting and I'll tell you if it's okay’ “—is “somewhat ridiculous.”

When Rich started at the FTC 26 years ago, the expansion of the internet as a commercial medium was just beginning, and the mobile market place was just emerging. Today, issues related to privacy and security are much more complex and the traditional notion of notice and consent—a “one-to-one understanding of ‘tell me what you're collecting and I'll tell you if it's okay’"—is “somewhat ridiculous,” Rich said.

Some connected devices don't even have an interface to disclose privacy policies to consumers, Rich said. As new technologies emerge, there are new types of information that need protection, including geolocation data, online credentials and content of communications, she said.

Moving forward, the commission must continue to keep pace with the technological changes, and companies need to voluntarily comply with basic privacy principles, Rich said. In addition to protection of data, Rich said that device security is another problematic issue to address. The dangers are no longer just data security, but actual physical danger, she said.

Many IoT devices, including pacemakers and automobiles, can be hacked and

remotely controlled, Rich said. She added that many connected devices that look “benign,” such as connected toys, could compromise the whole network by being used in a distributed denial of service attack, similar to the cyberattack in October 2016 that caused massive internet outages.

Privacy Shield Commitment

As the internet connects the world, international data transfer mechanisms will be “increasingly significant,” Rich said. Multinational companies and consumers alike want certainties and data protection worldwide, she said. To address this crucial aspect of international commerce, the FTC has a whole office devoted to international coordination and assistance, she said.

More than 4,400 U.S. business and European companies doing business with them relied on the U.S.-European Union Safe Harbor framework allowing trans-Atlantic commercial data transfers. Following the invalidation of the framework by the European Court of Justice for failing to sufficiently protect the privacy of EU subjects, negotiators reached a replacement deal, the EU-U.S. Privacy Shield. Whether the Privacy Shield is immune to the same fate as Safe Harbor is uncertain.

The FTC is “extremely committed” to the EU-U.S. Privacy Shield.

The FTC is “extremely committed” to the EU-U.S. Privacy Shield, which is stronger than the Safe Harbor, Rich told Bloomberg BNA. “We are poised to enforce it as we have enforced the Safe Harbor program” and “we are going to do everything to make it work,” she said.

Data Security Enforcement Authority

Rich defended the FTC's authority to pursue data security enforcement actions.

She played a central role in the FTC's data security enforcement action against hotelier Wyndham Worldwide Inc. that resulted in a federal appeals court ruling upholding the FTC's authority. Wyndham settled the action on remand

to the trial court.

Companies under FTC jurisdiction—from internet giants Amazon.com Inc. and Facebook Inc. to smaller businesses such as LabMD Inc.—have struggled with what level of data security they must provide in order to convince the nation's main data security and privacy enforcement agency that their efforts to protect personal data are reasonable. In the absence of direct data security statutory or regulatory authority, the FTC has relied on the Federal Trade Commission Act's Section 5, a catch-all prohibition on unfair and deceptive trade practices, to carry out data security compliance actions.

There are separate ongoing lawsuits in the U.S. Court of Appeals for the Eleventh Circuit and the U.S. District Court for the Northern District of California challenging the commission's authority. Companies challenging the agency's authority to bring actions “is not a new thing,” Rich said.

“We strongly believe not only do we have authority to pursue privacy and data security actions under the FTC Act, it's the right thing to continue to protect consumers,” Rich said.