Proskauer

With Regulators Increasing Focus on Spam Robocalls, Arkansas Follows Others States in Passing Anti-Spoofing Privacy Law

Privacy Law Blog on **April 8, 2019**

Unwanted robocalls reportedly totaled 26.3 billion calls in 2018, sparking more and more consumer complaints to the FCC and FTC and increased legislative and regulatory activity to combat the practice. Some automated calls are beneficial, such as school closing announcements, bank fraud warnings, and medical notifications, and some caller ID spoofing is justified, such as certain law enforcement or investigatory purposes and domestic violence shelter use. However, consumers have been inundated with spam calls – often with spoofed local area codes – that display fictitious caller ID information or circumvent caller ID technology in an effort to increase the likelihood consumers will answer or otherwise defraud consumers. To combat the rash of unwanted calls, Congress and federal regulators advanced several measures in 2019 and states have tightened their own telecommunications privacy laws in the past year. For example, within the last week, the Arkansas governor signed into law S.B. 514, which boosts criminal penalties for illegal call spoofing and creates an oversight process for telecommunications providers.

Even before this wave of regulatory and legislative attention, there were already a number of federal laws that sought to restrict certain unwanted calls, such as the Telephone Consumer Protection Act (TCPA), Truth in Caller ID Act, and various regulations surrounding the Do Not Call Registry and the Telemarketing Sales Rule, which, depending on the statute, are enforced by the FCC or FTC. In 2017, the FCC adopted rules to allow phone companies to proactively block illegal robocalls and, in February 2019, issued a proposed rulemaking to further combat illegal spoofed texts and international calls and a report on the regulatory and industry progress in combatting illegal robocalls. On the legislative front, within the last week, the Senate Commerce Committee favorably reported a bipartisan bill, S.151 (the TRACED Act), which would, among other things, increase the statute of limitations for FCC enforcement actions against illegal robocallers, require the FCC to promulgate rules regarding the blocking of unauthenticated calls and compel providers to take further actions to stem unwanted robocalls, including implementing the SHAKEN/STIR authentication framework, a technology that uses certificates to validate the source of each call.

On the state level, regulators and legislatures have also taken action, including the recently-passed Arkansas bill that increases protections under existing consumer protection statutes and bolsters criminal penalties for illegal call spoofing. The Arkansas law principally prohibits a person to "cause a caller identification service to transmit misleading or inaccurate caller identification information if the purpose is to defraud, cause harm, or wrongfully obtain anything of value" or use a third party to display or cause to be displayed spoofed caller ID information for any purpose, absent certain law enforcement and public safety exceptions. Moreover, telecommunication providers are required to report yearly to state regulators about how providers are implementing current technologies – such as SHAKEN/STIR – to block illegal robocalls. Arkansas's legislative action on call spoofing follows other states' enactments in the past year that have strengthened existing laws. For example, in 2018, South Carolina signed the "Telephone Privacy Protection Act," which, among other things, prohibited call or text spoofing, Louisiana passed S.B. 204, which enhanced remedies against caller ID spoofing, and Maryland passed the "Caller ID Spoofing Ban of 2018." Other states, including Illinois , Massachusetts and Ohio, among others, are currently debating bills that prohibit certain robocalling practices.

It remains to be seen whether the federal and state regulation and the adoption of authentication technology will curtail spam calls and texts. Entities transmitting automated calls or using caller ID spoofing for non-solicitation purposes should reexamine and monitor the changing legal landscape in this area.

View Original

Related Professionals

- **Laura E. Goldsmith**
  Partner