The race is on for medical device companies to develop mobile apps and network aware products. Whether or not these apps and products qualify as "mobile medical devices" under the FDA, however, will not diminish the potential for legal exposure to companies. Even for those apps that are not regulated by the FDA, there are substantial legal and compliance risks.

The plaintiffs' class action bar has aggressively pursued actions against major companies based on allegedly undisclosed collection and sharing of personally identifiable information ("PII") through mobile apps and network-aware devices, and there is no reason to believe that device makers will be spared. What makes the area so perilous is that PII no longer means just first and last name and Social Security Number, but can also mean technical information like unique identifiers, MAC address, device name, advertising identifiers, hardware serial numbers, identifiers associated with social networks, "hashed" information, geo-location coordinates, sensor output, and the list goes on and on. When this type of technical information is shared with 3rd parties: hosted solutions, mobile platforms, analytics providers, advertising parties, and vendors, media organizations and independent researchers "out" companies in major media outlets, on blogs, and on Twitter, claiming violations of end-user privacy. The regulatory investigations and class actions inevitably follow soon thereafter.

This webinar will take a deep dive into some mobile apps, look at how problematic data is collected and shared "behind-the-scenes," what it takes to be able to spot such collection, and what can be done in terms of mitigation (changing features, collection, or simply modifying disclosures). The focus will be on identifying real risks and practical solutions.

Presenter:
Steven Roosa, Co-Chair of the Privacy and Data Security Team at Holland & Knight. Steve is a partner in the firm and runs its internal privacy testing lab where he helps clients reduce and eliminate legal risks associated with data collection and sharing in mobile apps, websites, and network-connected devices. Steve is a fellow emeritus at the Center for Information Technology Policy (CITP) at Princeton University and co-author of "Trust Darknet: Control and Compromise in the Internet's Certificate Authority Model."