Gavel to Gavel: Wearable Tech and Privacy

Tom Wolfe is a trial attorney and commercial litigator whose practice is focused on complex business cases including product liability, oil and gas, mass tort and class action defense. Tom is also the president and managing partner at Phillips Murrah.

By Tom Wolfe, Published Nov 14, 2013 in The Journal Record monthly legal column, Gavel to Gavel.

Privacy and progress

We should have seen it coming. Maxwell Smart’s shoe phone heralded a future explosion of ubiquitous, wearable technologies.

Today, the landscape includes a growing assortment of inseparable, life-enhancing devices designed to help communicate, monitor, measure, and maintain our very existence. We’re more connected and better monitored than ever before, but at what risk to an individual’s privacy? Are our laws keeping pace with the enhanced capabilities of evolving technologies or are they holding back progress?

Generally, your rights and expectations of privacy are determined by your location. You have no expectation of privacy while standing in the middle of Disney World, but you have an extremely high expectation of privacy in the shower. Voluntarily putting oneself in public spaces generally defeats an expectation of privacy. The question remains as to whether putting yourself in a public space means you consent to being recorded, monitored or advertised to.

Some emerging wearable technologies are designed to appear like glasses, bracelets, watches or other unobtrusive accessories with the ability to record your activities or the world around you. One day you’re shopping down the vegetable aisle, the next you’re on a website called People of Walmart because you forgot you were wearing your favorite pair of leopard tights with a neon green sweat shirt. While being caught in that outfit may be embarrassing, your concern would be justifiably higher if you realized a stranger was recording video or taking pictures of your children.

On the more sinister side, as physicians use wireless versions of internal insulin pumps and pacemakers, security researchers

are concerned about possible cyberattacks on such implanted medical devices, so much so that former Vice President Dick Cheney took note.

What’s the expectation of supplying adequate security on these implants by the manufacturer? The good news is companies are already offering cybersecurity for medical devices, ranging from wireless frequency jammers for your pacemaker to ultrasound devices that determine where and when a malicious actor attempts to access your implant. The Food and Drug Administration is pushing medical device companies to increase security on their products.

At its current pace, technology seems to develop with the central idea that users want to record and share everything. This development doesn’t bode well for individual privacy.