Business & Careers

Wearable technology raising many legal concerns

Luigi Benetton

Towards the end of the dystopian 2013 satire *The Circle*, by Dave Eggers, the protagonist wears a front-facing wearable camera and microphone device that live-streams (except for bathroom breaks) her every waking moment to millions of followers.

In the real world, Toronto Police Services recently announced a pilot project consisting of distributing front-facing "body-worn" cameras to front-line officers. Toronto cops are following the lead of police forces elsewhere in Canada and the United States.

While stated reasons for this project are rational, the obvious Orwellian implications form the tip of a legal iceberg when it comes to wearable technology. And given increasing adoption rates of wearables by consumers, lawyers will want to know how these emerging and evolving technologies are used — and perhaps misused.

Experts figure current laws concerning the use of items like mobile phones and in-car touchscreens will provide largely adequate guidance when wearables appear in legal proceedings.

That's not to say new laws won't hit the books. David Canton, a technology lawyer with Harrison Pensa, notes that "lawmakers in the states of West Virginia and Delaware have already introduced bills to ban wearable computers while driving," in his paper *Wearable Computing: Legal Issues*, presented during last October's Canadian IT Law Association conference.

Various scenarios make for interesting thought experiments. Consider fitness trackers. I use both a Fitbit Flex and a Polar training computer. Were I an American, could health insurance companies require me to share tracker data to find out just how active I am compared to claims I made on insurance forms?

Returning to the camera scenario, could wearables supersede mobile phone cameras and be used to gather information to support a grievance against an employer?

To add a twist to the saying "putting a name to a face," facial recognition technologies may enable people wearing Google Glass to scan other people's faces, then search the Internet for images linked to faces (LinkedIn profiles could be a source) to return the person's name to the wearer of Glass.

The creep factor is undeniable. "I may no longer have practical anonymity in public spaces," says Timothy Banks, the Canadian lead for the privacy and security practice at Dentons Canada.

Questions like these are coming our way. People are moving "down the continuum from personal computers to mobile devices to wearable computers," Canton states in his paper.

Privacy may be the biggest legal concern. Mobile phones can already record video of anything happening around their users (just ask Toronto Mayor Rob Ford), but newer technologies like certain "smartwatches," body-worn cameras and the much-hyped Google Glass can do so more surreptitiously.

It may seem obvious, but it's still worth pointing out: when used, wearable devices gather data. If devices send that data to cloud-based servers, the result is sousveillance, in which the person who performs activities is the one who records them (e.g. recording the route of a run using a GPS-enabled device).

Gadget owners often intend to generate data about themselves. Banks, for instance, uses training computers when he runs. These gadgets "let you measure your activity, and then later look at them, compare them, to see objective results for your activities," he says.

MARTIN-MATTHEWS / ISTOCKPHOTO.COM

> "I may no longer have practical anonymity in public spaces.
>
> **Timothy Banks**
> Dentons Canada

Information typically goes to a cloud-based server for processing, to add value for the device owner. But doubt about how the server's owners use that information gives rise to what Canton refers to as the "mother ship" problem.

"What does the mother ship do with all that information?" he asks. "Do they use it for other things? How long do they keep it? The NSA/Snowden revelations make people really nervous about this stuff."

How much should we worry about who else sees this data? "At the risk of oversimplifying a complex subject, Canadian privacy laws require notice and consent for the collection, use and disclosure of personal information," Canton hedges in his paper.

Oversimplification is a real risk, given just how much data people generate and share via the cloud, and how that willingly shared information might leave them vulnerable to unwanted consequences. Stuff like photos, purchases, movements, interactions and other information led Canton to title one section of his paper "Behavioural Advertising and the 'Freaky Line.'"

Certain U.S. states have banned Google Glass over privacy concerns. "They don't want people filming everybody around them," says Chuck Rothman, director of e-discovery services at e-discovery and information governance firm Wortzmans. While he figures the specter of people-watching from cafés may be little more than fear-mongering, keeping Glass out of places like locker rooms seems a more legitimate goal.

Wearables might be seized and searched by law enforcement. Whether or not devices can be searched without warrants may depend upon whether said devices are locked.

Going a step further, wearables, or at least the data they generate, may enter the field of e-discovery. "I can envision somebody getting into a traffic accident wearing a medical monitoring device, and an insurance company may request that device to see what the person's medical condition was," says Rothman.

Medical issues may arise should people rely on self-help medical diagnostic devices that work with smartphones to make medical treatment decisions. Canton differentiates between such devices and fitness trackers. "If trackers don't get it quite right, it's not the end of the world. There isn't much liability there."

Rothman notes that certain medical devices transmit sensitive health information to a person's doctor. "That information could be intercepted," he says, noting that doctors might not be able to keep patient data confidential, as they're obliged to do.

Laws concerning wearable technology seem set to evolve over time, especially as new wearables hit the market. Banks notes that the concept of "privacy by design" is infiltrating the design departments of many device makers. This concept may prove more effective than mere privacy notices, which frequently languish unread.

"To think wearable technology will be banned or corralled by legal issues is a bit naïve," Canton says, adding that he hopes any debate will not stifle the advantages that these innovations bring.