Google Glass: Who's Watching YOU?

Lynne Williams, School of Business and Information Technology, 2014

Originally published on the "Industry Insights" section of the Kaplan University website.

Google Glass: Who's Watching YOU?

Mobile computing has been around now for over 30 years, arguably beginning with the Compaq© Portable "suitcase" computer back in 1982. The Portable weighed in at a hefty 28 lbs., not exactly the type of device that you'd forget you were carrying! Fast forward 3 decades and we are now surrounded by much smaller, lighter devices that easily fit in a pocket, or, in the case of Google Glass, on our nose.

Google Glass is a perfect example of Weiser's (1991) "ubiquitous computing" concept, which predicted an array of wearable devices aimed at providing the user with a range of location-based services and context-aware applications that would track the user's movements, ostensibly to aid that user as they moved through their environment. The fourth update (in late 2013) to Google Glass's capabilities allows a Glass user to keep track of dinner or concert reservations, stay posted on weather and traffic and conditions, and even the ability to search local movie theater showings and locations.

What concerns many observers is the fact that, while the user is keeping track of their Peter Frampton concert reservations or the gridlocked drive home, the Google Glass device is also keeping track of the user, as well as people and places in proximity to the user. What the wearer of a Google Glass sees can also be seen by others as the device streams video signal across the Internet. Google Glass takes us from ubiquitous computing to "ubiquitous surveillance" (The Economist, 2013). While Google currently bans the use of face recognition technology in any apps that it approves for use with Glass, the ban isn't likely to pose any barriers to hackers intent on using a Glass wearer as an unwitting spy. In December 2013, Lamda Labs, a development startup, released an unauthorized face recognition app for Glass that can be installed on the device by anyone willing to root the device and "side-load" the app (Greenberg, 2013b). Although the majority of potential users won't be willing to go that far to install such an app, it's an easy assumption that there will be a certain percentage of shadier types who will.

Lamda Labs developers are working on methods for cross-indexing user-supplied information about captured facial images, potentially enabling a user to not only log faces that have been recorded by the Glass device, but to also draw in information about the owner of a given face from a variety of sources, such as Facebook and LinkedIn. While advocates of this type of information collection might call it data mining, some privacy experts liken the possibility to linkage attacks, where seemingly innocuous information is drawn from a variety of sources to make a more detailed and revealing sum of the parts.

Given that Google has encouraged users to hack their Glass device (within Google mandates), it didn't take long for unforeseen consequences to appear. In May 2013, Lookout Mobile crafted a "QR photobomb" attack that uses malformed QR codes to misdirect the Glass device to a malicious wifi hotspot or to a website "designed to take full control of the device" (Greenberg, 2013a), with the user being none the wiser that their device had been hijacked. If a hijacked Glass device should also contain a stored log of images and any connections made to those images, it doesn't take much imagination to understand the potential for significant abuse of individual privacy.

Obviously, Google Glass is still a work in progress and the development team in charge of the Glass device has been responsive to the various findings coming in from individual and commercial Glass users. However, the troublesome aspect of Google Glass doesn't lie with its voluntary users, but in the innocent bystanders who are seen by those users. Now you see me… and now I am recorded and logged without consent, that's the issue.

References

Greenberg, A. (2013a). Google Glass Hacked With QR Code Photobombs. Forbes.Com, 10.

Greenberg, A. (2013b). Google Glass Face Recognition App Coming This Month, Whether Google Likes It Or Not. Forbes.Com, 13.

Every step you take. (2013). The Economist.

Weiss, T. R. (2013). Google Glass Update Bringing Movie, Dining, Traffic Info and More. Eweek, 5

Wieser, M. (1991). The Computer for the 21st Century. Scientific American, 10. doi: 10.1038/scientificamerican0991-94