Face, The Future

Public Expression in an Augmented World

By John C. Havens, author of Hacking H(app)iness – Why Your Personal Data Counts and How Tracking it Can Change the World and founder of The H(app)athon Project

Our 'face print' is one of our most unique identifiers and most of us continuously share it with others. Facial recognition combined with augmented reality and wearable display technologies like Google Glass or digital contact lenses will completely change how we (and others) see and use our faces. In the near future, our faces will allow people to see our identities and personal information floating before their eyes.

It also means these technologies will interpret our expressions. Wondering why that neighbor at Starbucks seems upset? Track their face and you might see their Facebook status was just changed to "single," or that they switched their LinkedIn status to "job seeker." Your lenses can also track your own expression, via eye tracking tools measuring your pupil's dilation as a correlation to emotion. Soon you'll start to see texts from your device with notes like, "Dude, you're scowling again. Your girlfriend's expression has an 88% ratio of frustration."

Beyond the privacy issues associated with our personal data, we need to begin thinking about the ethics and cultural changes these technologies will bring as I wrote in a piece for Mashable over a year ago, *The Impending Social Consequences of Augmented Reality*. Augmented reality, facial recognition, and artificial intelligence tech that personalize our lives provide great potential for advances in the fields of health, commerce, and our lives in general. But, to avoid negative legal or cultural repercussions in the future, *now* is the time to develop and advocate for guidelines or standards around how people and the information associated with them is tracked, accessed and used in the real world.

About this paper

The IEEE SA solicited the development of and obtained permission to distribute this position paper by John C. Havens for the purpose of initiating dialog with AR community members and experts.

Readers are encouraged to consider how they will adapt their behaviors in light of the likely scenarios.

To watch the IEEE-hosted Google+ Hangout panel discussion on this topic, visit https://plus.google.com/u/0/events/cb1gbpiigjv11rr6qjcc62nmd4s

The Facts to Face

"Facial recognition is absolutely inevitable." Russell S. King is CEO of Paycasso, a company that combines facial recognition and ID validation. As augmented reality-enabled devices become ubiquitous, it's solutions like the ones Paycasso provides that are creating precedents for how we'll manage our identities in public. "I personally feel our faces are an aspect of our identity that should be under our control," noted Russell in our interview, who is also participating in a multistakeholder process to develop a code of conduct on how the Consumer Privacy Bill of Rights applies to facial recognition technology. The fact that the National Telecommunications and Information Administration is creating the code reflects the growing

need for standards regarding how information is publically accessed via devices like Google Glass.

Currently legal precedents like copyright law favor individuals taking pictures and capturing publically available data versus the individuals whose images are being captured, tagged, and potentially sold without their knowledge or consent. It's this idea of our identities being bought and sold without transparency that provides a massive opportunity for change. The data broker industry, which makes multiple billions of dollars a year in revenue, currently doesn't allow U.S. consumers to even view data collected about their lives, let alone profit from it.

"The problem is that your face is quintessentially public. You can't help but share it." Brian Wassom is an expert on augmented reality law, and a partner at international business law firm Honigman Miller Schwartz and Cohn LLP. Wassom often writes about a legal term known as the right of publicity, which involves the ability for an individual to control the commercial exploitation of his or her personal identity. "Facial Recognition is a public domain issue so far," he noted in our interview, "but when it becomes the trigger for data collection and advertising then you're laying the groundwork for theories on how publicity rights should govern this behavior."

This right of publicity provides a critical opportunity for us to manage and protect our personal data before we lose the chance to control how our identity is broadcast in the future. This could mean as we walk around the physical world others could view a completely different virtual person via the digital doppelgangers advertisers project reflecting our identity.

More likely, our view of the world will be dictated by the mobile network operators who we pay to keep data flowing to the devices we wear, a troubling possibility in the wake of the recent ruling on Net Neutrality. A legal principle allowing for unrestricted access for users to the Internet despite their data coming from any specific carrier, Net Neutrality used to keep cable and phone companies from being able to slow down or block certain websites. But when our lives are portrayed in the form of digital data via augmented reality, this new ruling sets a precedent where individuals may not be portrayed in people's field of vision based on their carrier or device.

"Augmented content has to come from somewhere," says Wassom. "Companies will be controlling the pipes (for our data) which means AR-based experiences may not be as democratic and universal as we'd like to think."

Clouding Our Perspective

Managing exposure to these technologies boils down to how a person wishes to protect, utilize, and share their data. In an augmented world where images provide cues for digital data to present itself, people need ways to better manage their data. Personal Clouds, part of an industry and trend Forrester Research has dubbed Personal Identity Management, provide the best opportunity for this type of individualized control. The basic idea of these Clouds is analogous to how you manage your money in a bank account – you lock it and only you can control who accesses it and when ("Clouds" are also sometimes referred to as "Personal Data Vaults" or "Banks"). This means that the "Golden Copy" of your most precious data, your PII,

(personally identifiable information) can be set up in such a way that the government, businesses, or anyone else only receive the information you want to provide for whatever transactions you allow.

"But it's not necessarily your data itself that has value – when an individual is brought into the relationship, it's the *relationship* that has value." Drummond Reed is CEO of Respect Network, a global organization founded in 2011 to build "the world's first personal cloud network." *(Disclosure – my non-profit foundation, The H(app)athon Project, is a Founding Partner in Respect Network).* Personal Clouds in this network will allow people to safely store and share their data however and with whomever they want. Like a Dropbox on steroids, they'll offer one of the only alternatives to the free-for-all data access model that currently drives the digital world.

"Data brokers exist because there has not been any efficient or trusted way for people to share data with businesses directly," noted Reed in our interview, pointing out the need for Personal Clouds that let users take control over their relationships with other individuals as well as businesses. It's a paradigm that moves the conversation beyond how much our data is worth to redefining the worth of our data.

A Data in the Life

For an example of how people could interact within the augmented reality/Personal Cloud paradigm of the future, I've included an excerpt from my current book, *Hacking H(app)iness – Why Your Personal Data Counts and How Tracking it Can Change the World:*

> You're at a Starbucks waiting in line and get an IM (instant message) in your HUD (heads-up display—like Google Glass, but it covers both your eyes). A camera icon with a question mark appears in the upper right-hand portion of your vision, meaning someone nearby wants to take a picture and you're in the shot. You IM back an automated message:
>
> *Hi. Looks like you want to take a picture that would feature my image. Since we're in a public space, I can't keep you from snapping. But if you use facial recognition to tag me, note that I own my own data in any format and will appear as an avatar in your picture unless you receive my written consent to use my image.*
>
> You immediately get another IM with a money icon and a URL link to a blog. You blink to open the URL and see a series of riveting black-and-white photographs featuring people waiting in lines. The title of the blog is *This Is Your Queue*, and you think it's really cool. So you blink on the money icon and a message appears from the person requesting the picture that says:
>
> *I use PaySwarm to provide micropayments for anyone I feature in my images. I don't tag people's faces, and I have a computer program that constantly scans the Web to make sure other people aren't using my pictures without permission. So if*

> *you let me use your image, your visual data will be safe, and after a while maybe you'll make enough money to buy a coffee like the one you're waiting in line for right now.*
>
> You blink twice toward the IM to accept these conditions, looking to the right using eye-tracking technology to save the URL for the blog so you can check it out in the future. You turn and smile at the photographer who has identified himself sitting nearby, appreciating the fact your picture has become a work of art.

The User as Chooser

What will it take for the scenario above to come about? Today, when a person takes a picture in public we know it. They raise their phone or camera at a group of people who smile and stand still. These are the culturally accepted norms that let us know someone is taking a picture. We may also be videotaped or photographed without our knowledge, either by government or private actors we may or may not trust. Beyond our faces, our cars and bodies are also tracked via RFID and other sensor technology proliferating via the Internet of Things.

These technologies will continue to proliferate, which means creating consensus-based systems around us and requesting that the companies creating the tech or broadcasting our data comply with those will be an ongoing struggle. The balance we define between growing the profits of businesses versus individual user control of something as basic as their face print will be of paramount importance. Personal Clouds provide a solution for managing data that will not stymie commerce or innovation, but will allow whole new economies to prosper built on trust. What are other solutions? How will people become more adept at developing their personal privacy policy? A person's preference towards privacy can be managed however they wish, while greater transparency and economic gain will also increase for the general population as a whole. We must move into the future with the Personal Cloud paradigm in place to have an Augmented World we can look forward to seeing.