Unintended, malicious and evil applications of augmented reality

by Gregory Conti, Edward Sobiesk, Paul Anderson, Steven Billington, Alex Farmer, Cory Kirk, Patrick Shaffer, and Kyle Stammer

Most new products begin life with a marketing pitch that extols the product's virtues. A similarly optimistic property holds in user-centered design, where most books and classes take for granted that interface designers are out to help the user. Users themselves are assumed to be good natured, upstanding citizens somewhere out of the Leave it to Beaver universe.

In reality, however, the opposite is often true. Products have substantial flaws, technology designers seek ways to extract money from users, and many users twist well-intentioned technology in ways the designers never expected, often involving baser instincts.

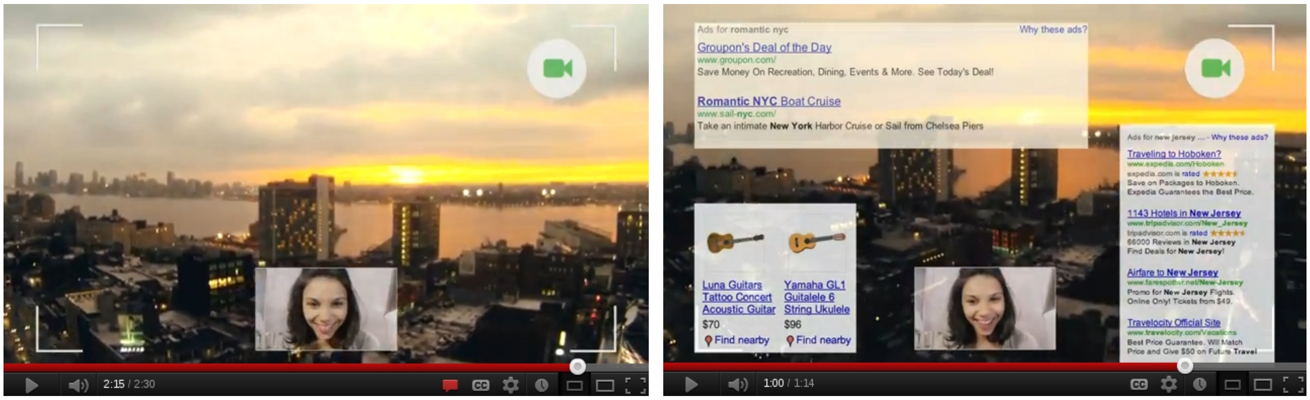
These realities should come as no surprise to security professionals who are usually most effective when assuming the worst of people. One sure to be abused emerging technology is augmented reality.

Augmented reality technologies overlay computer generated data on a live view of the real world.

Anticipated application domains include entertainment, travel, education, collaboration, and law enforcement, among numerous others.

Augmented reality bears great promise as exemplified by Google's highly optimistic "Project Glass: One day..." video. In the video, a theoretical descendent of Google's Project Glass helps the user navigate a city, communicate, learn the weather, and otherwise manage his day.

A day after Google posted the video, YouTube user rebelliouspixels posted a parody video "ADmented Reality" that remixed Google's Project Glass vision with Google Ads. As we look to the future, this less optimistic view likely will be closer to the mark.



Ads for romantic nyc

Why these ads?

Groupon's Deal of the Day
www.groupon.com/
Save Money On Recreation, Dining, Events & More. See Today's Deal!

Romantic NYC Boat Cruise
www.sail-nyc.com/
Take an intimate **New York** Harbor Cruise or Sail from Chelsea Piers

Luna Guitars Tattoo Concert Acoustic Guitar
$70
Find nearby

Yamaha GL1 Guitalele 6 String Ukulele
$96
Find nearby

Ads for new jersey .... - Why these ads?

Traveling to Hoboken?
www.expedia.com/Hoboken
expedia.com is rated ★★★★★
Save on Packages to Hoboken.
Expedia Guarantees the Best Price.

1143 Hotels in **New Jersey**
www.tripadvisor.com/New_Jersey
tripadvisor.com is rated ★★★★★
66000 Reviews in **New Jersey**
Find Deals for **New Jersey**!

Airfare to **New Jersey**
www.farespotter.net/New-Jersey
Promo for **New Jersey** Flights.
Online Only! Tickets from $49.

Travelocity Official Site
www.travelocity.com/Vacations
Best Price Guarantee. Will Match
Price and Give $50 on Future **Travel**

Optimistic view of future augmented reality as envisioned by Google (left). A more pragmatic, and advertisement laden, view by YouTube user rebelliouspixels (right).

In this article, we combine augmented reality with reasonable assumptions of technological advancement, business incentives, and human nature to present less optimistic - but more probable - future augmented reality applications.

Admittedly, some are dystopian. We end with suggestions for the security and usability communities to consider now - so that we may be better prepared for our future of augmented reality and the threats and opportunities it presents.

We do not intend to propose science fiction, but instead consider technologies available today or likely to arrive in the next five to ten years.

Unless otherwise stated, we assume the capabilities and overall popularity of today's iPhone/iPad - always on networking, high resolution video cameras, microphones, audio, voice recognition, location awareness, ability to run third-party applications, and processing support from back-end cloud services - but resident in a lightweight set of eyewear with an integrated heads-up display.

Learning from the past

As we consider potential misuse and risks associated with augmented reality we can learn a great deal from past desktop applications and current iPhone and Android apps to gain insight into both human nature and technical possibilities. From this analysis we identify at least three primary threat categories.

The first category is simplest, current applications that are easily ported to future systems, with little to no augmentation.

The next category includes hybrid threats that are likely to evolve due to enhanced capabilities provided by augmented reality.

The final category, and the hardest to predict, are entirely new applications which have little similarity to current applications. These threats will lean heavily on new capabilities and have the potential to revolutionize misuse.

In particular, these applications will spring from widespread use, always on sensing, high speed network connectivity to cloud based data sources and, perhaps most importantly, the integration of an ever present heads-up display that current cell phones and tablets lack.

Regardless to which category the new threats belong, we assume that human nature and its puerile and baser aspects will remain constant, acting as a driving force for the inception of numerous malicious or inappropriate applications.

Applications

This section lists potential misuse applications for augmented reality. Of course, we do not mean to imply that Google or any other company would endorse or support these applications, but such applications will likely be in our augmented future nonetheless.

Persistent cyber bullying

In the world defined by Google Glasses users are given unparalleled customizability of digital information overlaid on top of the physical environment. Through these glasses this information gains an anchor into the physical space and allows associations that other individuals can also view, share, vote on, and interact with just as they would via comments on YouTube, Facebook, or restaurant review sites.

Persistent virtual tagging opens up the possibility of graffiti or digital art overlaid upon physical objects, but only seen through the glasses. However, hateful or hurtful information could just as easily be shared among groups (imagine what the local fraternity could come up with) or widely published to greater audiences just as it can today, but gains an increasing degree of severity when labeling becomes a persistent part of physical interactions.

Imagine comments like “Probably on her period” or “Her husband is cheating” being part of what appears above your head or in a friend’s glasses without your knowledge. Such abuse isn’t limited to adult users.

The propensity for middle and high school age youth to play games that embarrass others is something to be expected. The bright future predicted by Google may be tainted by virtual “kick me” signs on the backs of others which float behind them in the digital realm.

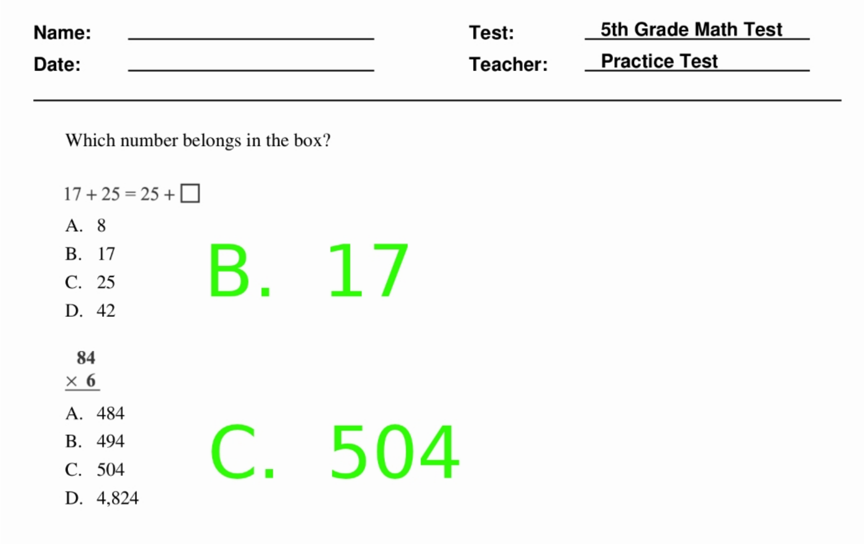
Lie detection and assisted lying

Augmented reality glasses will likely include lie detection applications that monitor people and look for common signs of deception. According to research by Frank Enos of Columbia University, the average person performs worse than chance at detecting lies based on speech patterns and automated systems perform better than chance. Augmented reality can exploit this. The glasses could conduct voice stress analysis and detect micro-expressions in the target’s face such as eye dilation or blushing.

Micro-expressions are very fleeting, occurring in 1/15 of a second, beyond the capabilities of human perception. However, augmented reality systems could detect these fleeting expressions and help determine those attempting to hide the truth. An implication is that people who use this application will become aware of most lies told to them. It could also provide a market for applications that help a person lie.

Cheating

Gamblers, students, and everyday people will likely use augmented reality to gain an unfair advantage in games of chance or tests of skill. Gamblers could have augmented reality applications that will count cards, assist in following the “money card” in Three Card Monte, or provide real-time odds assessments. Students could use future cheating applications to look at exam questions and immediately see the answers.



Name: ______________________ Test: 5th Grade Math Test

Date: ______________________ Teacher: Practice Test

Which number belongs in the box?

$17 + 25 = 25 + \square$

A. 8
B. 17
C. 25
D. 42

B. 17

$$\begin{array}{r} 84 \\ \times\ 6 \\ \hline \end{array}$$

A. 484
B. 494
C. 504
D. 4,824

C. 504

Future augmented reality applications will likely assist cheating. In this notional example the student sees the answers by simply looking at the test.

Stealing

Theft and other related crimes may also be facilitated by augmented reality. For example, persistent tagging and change detection could be used to identify homes where the occupants are away on vacation. We anticipate augmented reality will perform at levels above human perception. Applications could notice unlocked cars or windows and alert the potential criminal.

When faced with a new type of security system, the application could suggest techniques to bypass the device, a perverted twist on workplace training. The Google Glass video depicted the user calling up a map to find a desired section of a book store. We anticipate similar applications that might provide escape routes and locations of surveillance cameras.

Law enforcement detection

We also anticipate other applications to support law breaking activities. Today's radar and laser detectors may feed data into drivers' glasses as well as collaboratively generated data provided by other drivers about locations of traffic cameras and speed traps. Newer sensors, such as thermal imaging, may allow drivers to see police cars hidden in the bushes a mile down the road. License plate readers and other machine vision approaches will help unmask undercover police cars. Counter law enforcement applications will certainly move beyond just driving applications and may assist in recognizing undercover or off duty police officers, or even people in witness protection programs.

Front and rear looking cameras would allow users to see behind them and collaborative or illicit sharing of video feeds would allow users to see around corners and behind walls. Average citizens may use their glasses to record encounters with police, both good and bad.

Law enforcement

Law enforcement variants of augmented reality may dramatically change the interaction between police officers and citizens. The civil liberties we enjoy today, such as freedom of speech and protection against self-incrimination, will certainly be affected by impending augmented reality technology. What might be relatively private today (such as our identity, current location, or recent activity) will be much more difficult to keep private in a world filled with devices like Google Glasses.

A key enabler of future augmented reality systems is facial recognition. Currently, facial recognition technology is in a developmental stage, and only established at national borders or other areas of high security.

Ralph Gross, a researcher at the Carnegie Mellon Robotics Institute, claims that current facial recognition technology is becoming more capable of recognizing frontal faces, but struggles with profile recognition. Current technology also has problems recognizing faces in poor lighting and low resolution.

However, we anticipate significant advances during the next decade. Law enforcement agencies, like the police department in Tampa, Florida, have tested facial recognition monitors in areas with higher crime rates, with limited success. The primary cause behind these failures has been the inability to capture a frontal, well lit, high resolution image of the subject. This obstacle blocking effective facial recognition would be quickly removed in a world where augmented reality glasses are common and facial images are constantly being captured in everyday interactions.

While facial recognition via augmented reality (through glasses or mobile devices) might seem harmless at first glance, a deeper look into this new technology reveals important unintended consequences. For example, a new form of profiling may emerge as a police officer wearing augmented reality glasses might recognize individuals with prior criminal records for which the subjects have already served their time. Without augmented reality, that police officer would have likely never recognized the offenders or known of their crimes.

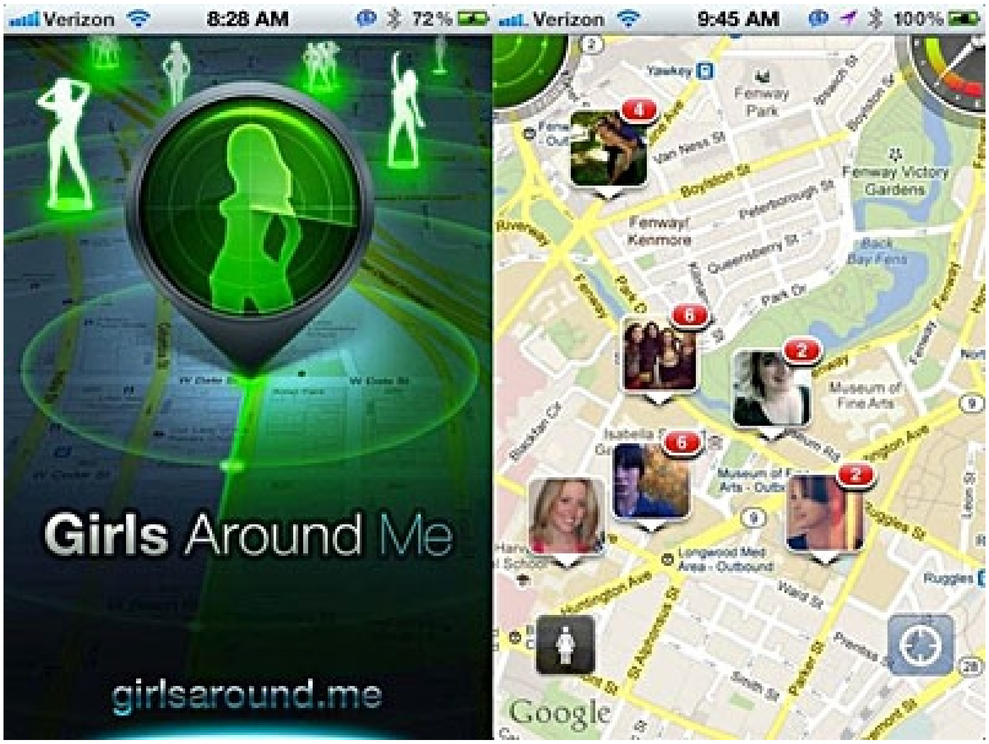
Of course augmented reality may be very beneficial to law enforcement activities, but raises serious questions about due process, civil liberties, and privacy. The end result may be a chilling effect on the population as a whole, both guilty and innocent.

Dating and stalking

Augmented reality opens the flood gates to applications for dating and stalking. Having a set of eyeglasses that records and posts your location on social networks means that everybody you know can see where you are. For example, a man sits down at a bar and looks at another women through his glasses, and her Facebook or Google+ page pops up on his screen (since she did not know to limit her privacy settings).

While augmented reality brings vastly new and exciting opportunities, the technology threatens to eliminate the classic way of meeting and getting to know people: by actually spending time with them.

Consider an application that already exists: “Girls Around Me”. Girls Around Me uses data from social networking sites to display locations of nearby girls on a map. According to Nick Bilton of The New York Times, this application “definitely wins the prize for too creepy.”



The “Girls Around Me” app for smart phones, which uses social networking data to locate nearby women, portends a future of creepy, but plausible augmented reality uses.

The evolution of such applications combined with augmented reality opens up numerous other possibilities. Perhaps the glasses will suggest pick-up lines based on a target’s interests, guess people’s ages, highlight single women (or married women), make people more attractive (virtual “beer goggles”), or provide “ratings” based on other users’ feedback. Lie detection applications will likely be in frequent use, and misuse. Expect continuous innovation in this domain.

Recreational pharma

We anticipate that augmented reality will be used to emulate or enhance drug use. History has taught us recreational drugs will always be in demand as will be additional means of enhancement. Some may recall the combination of drugs with Pink Floyd laser light shows.

Others may have experimented with Maker SHED’s Trip Glasses which suggests users “Enjoy the hallucinations as you drift into deep meditation, ponder your inner world, and then come out after the 14-minute program feeling fabulous” or the audio approaches suggested by Brad Smith’s DEFCON 18 “Weaponizing Lady GaGa” talk. Augmented reality will open up significant and sought after possibilities.

Erotica

Let's face it, porn is a driving force behind Internet and technological growth, and we believe the same will hold true for augmented reality.

Augmented reality will facilitate sexual activities in untold ways including virtual sexual liaisons, both physical and virtual, local and at a distance.

Advanced sensors may allow penetration of clothing or the overlay of exceptionally endowed features on individuals in the real world, perhaps without their knowledge. The advice frequently given in public speaking classes, "Imagine the audience naked," takes on entirely new meaning in this era.

Surveillance

There are more than 300 million people in the United States alone and more than that number of mobile phones. Imagine if even one third of this group actively wore and used augmented reality glasses. That would mean 100 million always-on cameras and microphones wielded by adults, teenagers, and children continually feeding data to cloud-based processors.

Virtually no aspect of day-to-day life will be exempt from the all seeing eye of ubiquitous and crowdsourced surveillance. Businesses will be incentivized to collect, retain, and mine these data flows to support business objectives, such as targeted advertising, and governments will covet and seek access to this data for security and law enforcement aims.

The implications of the privacy of the individual citizen and the chilling effect on society as a whole could be profound.

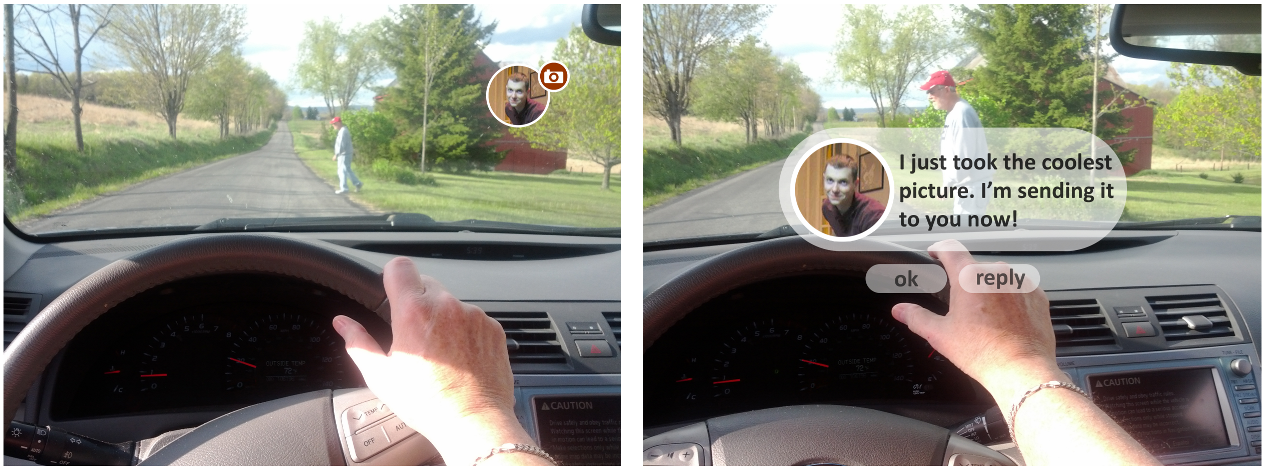
Distraction

People have long been concerned about the danger of billboards when driving, because they take drivers' eyes off the road. Text messaging while driving is widely illegal because of the distraction it causes.

Now consider augmented reality glasses with pop-up messages that appear while a person drives, walks across a busy intersection, or performs some other activity requiring their full attention.

For anybody wearing the glasses, text messaging or advertising alerts and similar interruptions would be very distracting and dangerous. You've likely seen, on many occasions, drivers attempting to use their cell phones and their resultant erratic driving.

Augmented reality devices encourage such "multitasking" behavior at inappropriate times. The results will not be pretty. Consider the example below of a driver reading a text message while a pedestrian is crossing the road.



Driver wearing augmented reality glasses receives text message and is too distracted to notice a pedestrian crossing street.

Voyeurism

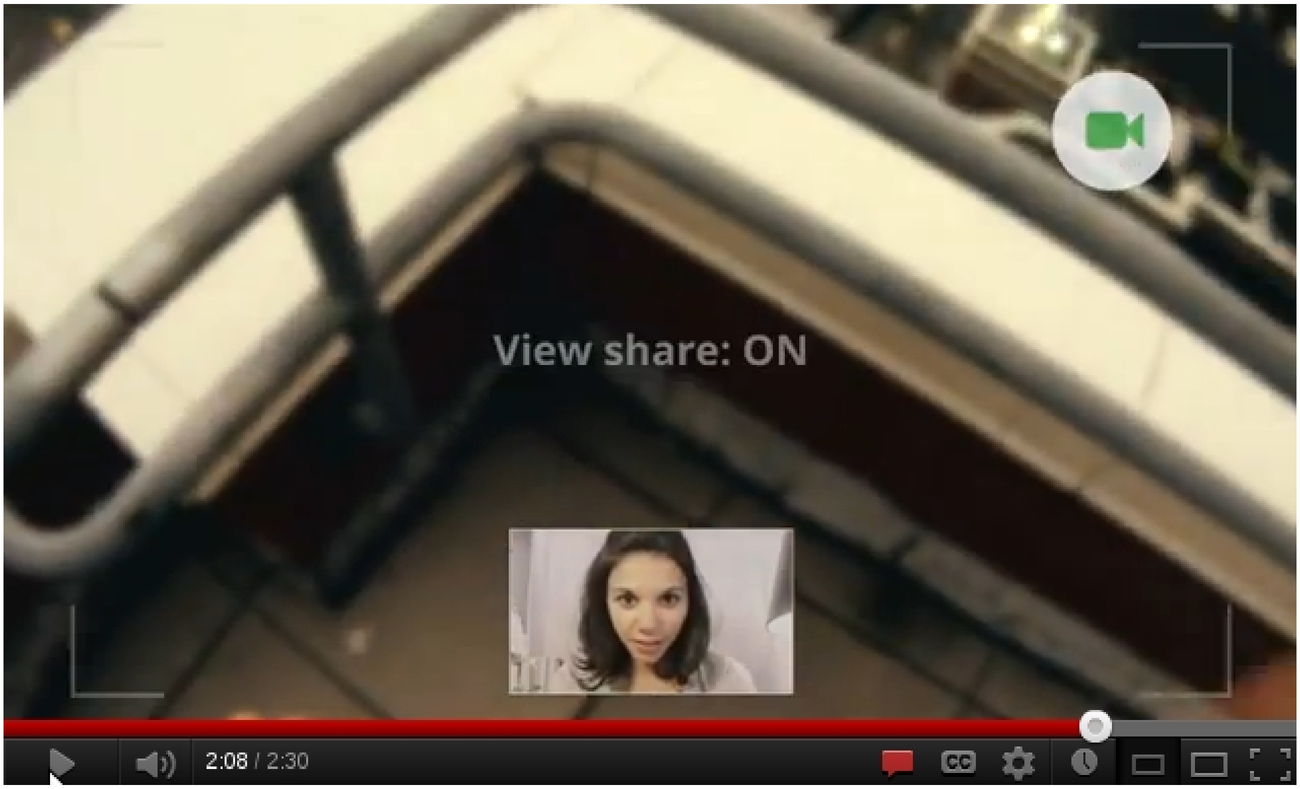
People today do stupid things (see the movie Jackass for textbook examples), and in the future, people will continue to do stupid things while wearing augmented reality glasses. One commenter on Google's YouTube video, PriorityOfVengence1, suggested that someone might even commit suicide wearing Google Glasses.

Man: Hey, wanna see something cool?
Girl: Sure!
Man jumps off building

The context of this comment refers to the end of the video when the main character is on a roof video chatting with his girlfriend and says "Wanna see something cool?"

PriorityOfVengence1's comment received over sixty thumbs up in just three days. While some might laugh at the comment, it highlights a disturbing potential reality.

What if people spiraling into depression began streaming their suicide attempts by way of their glasses? It is certainly possible - this and many other variations of augmented reality voyeurism should be anticipated.



In the Google Glasses video the main character stands near the edge of a balcony in a live video chat with his girlfriend. One YouTube commenter suggested Google Glasses might be worn while attempting suicide.

Untrusted reality

The focus of this article is on user applications that behave in accordance with the user's wishes. However, if we expand our assumptions to allow for malicious software, options become even more interesting. With malicious software on the augmented reality device, we lose all trust in the "reality" that it presents.

The possibilities are legion, so we will only suggest a few. The glasses could appear to be off, but are actually sharing a live video and audio feed. An oncoming car could be made to disappear while the user is crossing the street. False data could be projected over users' heads, such as a spoofed facial recognition match from a sexual offender registry.

For related malware research on today's mobile technology see Percoco and Papathanasiou's "This is not the droid you're looking for..." from DEFCON 18 to begin envisioning additional possibilities.

Conclusions

The era of ubiquitous augmented reality is rapidly approaching and with it amazing potential and unprecedented risk. The baser side of human nature is unlikely to change nor the profit oriented incentives of industry. Expect the wondrous, the compelling, and the creepy. We will see all three.

However, we shouldn’t have to abdicate our citizenship in the 21st century and live in a cabin in Montana to avoid the risks augmented reality poses.

As security professionals we must go into this era with eyes wide open, take the time to understand the technology our tribe is building, and start considering the implications to our personal and professional lives before augmented reality is fully upon us. To live in the 21st century today online access, social networking presence, and instant connectivity are near necessities.

The time may come when always on augmented reality systems such as Google Glasses are a necessity to function in society; before that time however we must get ahead of the coming problems. The first few kids who walk into their SAT exams wearing augmented reality glasses and literally see the answers are going to open Pandora’s Box.

Gregory Conti is Director of West Point’s Cyber Research Center and an Associate Professor of Computer Science. He is an active researcher in usable security, security data visualization, online privacy, and cyber warfare.

Edward Sobiesk is Director of West Point’s Information Technology Program and an Associate Professor of Computer Science. His research interests include electronic privacy, usable security, and computing education.

Paul Anderson, Alex Farmer, Patrick Shaffer, and Kyle Stammer are recent graduates of West Point where they studied computer science and information technology.

Steven Billington and Cory Kirk are currently seniors at West Point where they are studying computer science and information technology.

The views in this article are the authors’ and do not reflect the official policy or position of the US Military Academy, the Department of the Army, the Department of Defense, or the US Government.