Cameras to Detect ‘Abnormal’ Behavior

In the chimerical pursuit of perfect security, Western countries are turning to advanced technology to detect and stop terrorist attacks. But these expensive schemes often fail to deliver greater safety while further eroding personal freedom, as Sander Venema observed in the Netherlands.

By Sander Venema

A few days ago I read an article about how TNO (the Dutch Organization for Applied Scientific Research, the largest research institute in the Netherlands) developed technology for smart cameras for use at Amsterdam Schiphol Airport. These cameras — installed at Schiphol airport by the Qubit Visual Intelligence, a company from The Hague — are designed to recognize certain “suspicious behavior,” such as running, waving your arms, or sweating.

Curiously enough, these are all things that are commonly found in the stressful environment that an international airport is to many people. People need to get to the gate on time, which may require running (especially if you arrived at Schiphol by train, which in the Netherlands is notoriously unreliable); they may be afraid of flying and trying to get their nerves under control; and airports are also places where friends and family meet after long times abroad, which (if you want to hug each other) requires arm waving.

I suspect that a lot of false positives are going to occur with this technology due to this. It’s the wrong technology at the wrong place. I fully understand the need for airport security, and we all want a safe environment for both passengers and crew. Flights need to operate under safe conditions. What I don’t understand is the mentality that every single risk in life needs to be minimized away by government agencies and combated with technology. More technology does not equal safer airports.

Security Theatre

A lot of the measures taken at airports constitute security theatre. This means that the measures are mostly ineffective against real threats, and serve mostly for show. The problem with automatic profiling, which is what this program tries to do as well, is that it doesn’t work. Security expert Bruce Schneier has written extensively about this, and I encourage you to read his 2010 essay “Profiling Makes Us Less Safe” about the specific case of air travel security.

The first problem is that terrorists don’t fit a specific profile or they can carefully avoid “suspicious” actions. Thus, these profiling systems can be circumvented once people figure out how, and because of the over-reliance on
technology instead of common sense this can actually cause more insecurity.

In the novel *Little Brother*, Cory Doctorow wrote about how Marcus Yallow put gravel in his shoes to fool the gait-recognizing cameras at his high school so he and his friends could sneak out to play a game outside. Similar things will be done to try and fool these “smart” cameras, but the consequences can be much greater.

We are actually more secure when we randomly select people instead of relying on a specific threat profile or behavioral profile to select who to screen and who gets through security without secondary screening. The whole point of random screening is that it’s random. Therefore, a potential terrorist cannot in advance know what the criteria are that will make the system pick him out. If a system does use specific criteria, and the security of the system depends on the criteria themselves being secret, that would mean that someone would just have to observe the system for long enough to find out what the criteria are.

Technology may fail, which is something people don’t always realize. Another TNO report entitled: “*Afwijkend Gedrag*” (Abnormal Behavior) states under the (admittedly tiny) section that deals with privacy concerns that collecting data about abnormal behavior of people is ethically just because the society as a whole can be made safer with this data and associated technology. It also states (and this is an argument I’ve read elsewhere as well), that “society has chosen that safety and security trumps privacy.”

Now, let’s say for the sake of the argument that this might be true in a general sense (although it can be debated whether this is always the case, personally I don’t think so, as sometimes the costs are just too high and we need to keep a free and democratic society after all). The problem here is that the way technology and security systems are implemented is usually not something we as a society get to first have a vote on before the (no doubt highly lucrative) contracts get signed.

In the Dutch airport case, Qubit probably saw a way to make a quick buck by talking the Schiphol leadership and/or the government (as the Dutch state holds 69.77 percent of the Schiphol shares) into buying their technology. It’s not something the people had a conscious debate on, and then subsequently made a well-informed decision.

**Major Privacy Issues**

We have established that these systems are ineffective and can be circumvented (like any system can), and won’t improve overall security. But much more importantly, there are major privacy issues with this technology. What Schiphol
and Qubit are doing here is analyzing and storing data on millions of passengers, the overwhelmingly vast majority of whom are completely innocent. This is like shooting a mosquito with a bazooka.

What happens with this data? We don’t know, and we have to believe Qubit and Schiphol on their word that data about non-suspect members of the public gets deleted. However, in light of recent events where it seems convenient to collect and store as much data about people as possible, I highly doubt any deletions will actually happen.

And the sad thing is: in the Netherlands the Ministry of Security and Justice is now talking about implementing the above-mentioned behavioral analysis system at another (secret) location in the Netherlands. Are we all human guinea pigs ready to be tested and played around with?

**What Is Abnormal?**

There are also problems with the definitions. This is something I see again and again with privacy-infringing projects like this. What constitutes “abnormal behavior”? Who gets to decide on that and who controls what is abnormal behavior and what isn’t?

Maybe, in the not-too-distant future, the meaning of the word “abnormal” begins to shift, and begins to mean “not like us,” for some definition of “us.” George Orwell mentioned this effect in his book *Nineteen-Eighty-Four*, where ubiquitous telescreens watch and analyze your every move and one can never be sure what are criminal thoughts and what aren’t.

In 2009, when the European research project INDECT got funded by the European Union, there were critical questions asked to the European Commission by the European Parliament. More precisely, this was asked:

**Question from EP:** How does the Commission define the term abnormal behavior used in the program?

**Answer from EC:** As to the precise questions, the Commission would like to clarify that the term behavior or abnormal behavior is not defined by the Commission. It is up to applying consortia to do so when submitting a proposal, where each of the different projects aims at improving the operational efficiency of law enforcement services, by providing novel technical assistance. [Source: Europarl (Written questions by Alexander Alvaro (ALDE) to the Commission)]

In other words: according to the European Commission it depends on the individual projects, which all happen to be vague about their exact definitions.
And when you don’t pin down definitions like this (and anchor them in law so that powerful governments and corporations that oversee these systems can be held to account!), these can be changed over time when a new leadership comes to power, either within the corporation in control over the technology, or within government.

This is a danger that is often overlooked. There is no guarantee that we will always live in a democratic and free society, and the best defense against abuse of power is to make sure that those in power have as little data about you as possible.

Keeping these definitions vague is a major tactic in scaring people into submission. This has the inherent danger of legislative mission creep. A measure that once was implemented for one specific purpose soon gets used for another if the opportunity presents itself.

Once it is observed that people are getting arrested for seemingly innocent things, many people (sub)consciously adjust their own behavior. It works similarly with free speech: once certain opinions and utterances are deemed against the law, and are acted upon by law enforcement, many people start thinking twice about what they say and write. They start to self-censor, and this erodes people’s freedom to the point where we slowly shift into a technocratic Orwellian nightmare. And when we wake up it will already be too late to turn the tide.

Sander Venema is an experienced Web-developer and programmer who is concerned about the fast-emerging surveillance states which undermine civil liberties and human rights. He is also the founder of Asteroid Interactive, a Web design and development company based in The Netherlands. [A version of this story was originally posted at http://sandervenema.ch/]