

About...

Software, Surveillance, Scarieness, Subjectivity (and SVEN)

Amy Alexander
Department of Visual Arts, University
of California, San Diego
9500 Gilman Dr. #0084
La Jolla, CA 92093-0084 USA

ABSTRACT

The following text discusses cultural and political implications of the subjective aspects of software. It is adapted from a text that appears on the website of the SVEN project (<http://deproramming.us/sven>). SVEN is a public space software art project that uses custom computer vision software to detect pedestrians who in some way “look like” rock stars. The text introduces general audiences to SVEN’s approach to software subjectivity – in this case, concerning computer vision surveillance software.

1. INTRODUCTION

SVEN is a project developed by Amy Alexander, Jesse Gilbert, Wojciech Kosma, Vincent Rabaud and Nikhil Rasiwasia. The following text focuses on SVEN’s approach to and issues surrounding computer vision. Cinematography, and its relationship to both software and surveillance video, is also important to SVEN - but it’s a topic for a different text. Art is of course of particular importance to SVEN – but that should go without saying.

SVEN is a piece of tactical software art. Tactical software art comes out of traditions of tactical media and software art. It’s a logical mix: tactical media is a response to the way mainstream media influences culture; software art is a response to the ways mainstream software influences culture.

Tactical media often involves a combination of digital actions and “meatspace” – or street - actions. In SVEN, these are one and the same - digital actions that take place on the street (just off the curb in this case).

2. SURVEILLANCE IS ALREADY SCARY.

Sure, surveillance is scary - but you’ve probably heard that before. We’re being watched all the time, and we don’t know by whom, or what they’re doing with the images and other data they’re

gathering. Scared? You bet - there’s a bogeyman under the bed, so we’d better not look. But remember, we’re supposed to be scared – people are trying to scare us. Foucault pointed out that not knowing when the bogeyman is watching you can scare you into changing your behavior. But not knowing how the bogeyman is watching you can scare you too. SVEN’s purpose is not to point out that surveillance is scary. People are scared enough as it is.

3. SOFTWARE SHOULDN’T BE SCARY.

Technology as a big black box scares people into not looking at it. It’s all-powerful and incomprehensible. So often, people don’t question how it works:

An article from *WikiWikiWeb* entitled “Hermetically Sealed Stuff Is Magic” reads:

This is a principle of human nature pointed out to me by ScottAdams and his PointyHairedBoss. There is a Dilbert strip where the PointyHairedBoss works out a schedule for Dilbert, and bases it on the assumption that anything he cannot understand is easy (magic). Thus, he commands the poor drone to build a worldwide networking system in six minutes.

If you can understand something, you can reasonably evaluate it. If you can’t understand it (either it is beyond your comprehension, or someone has “hermetically sealed” it so you can’t see), you can’t reasonably evaluate it. (WikiWikiWeb)

That might sound at first like a geek-elitist position, implying that everyone should be a programmer and that those who don’t program are [lazy/stupid/inferior]. I can’t speak for the authors of that wiki article, but my point here is not to suggest that everyone learn to program, but rather that perhaps everyone should learn about programming. Think of software literacy as an extension of media literacy. People are (hopefully) taught how to detect bias in newspapers and television – even if they don’t know how to

produce a newspaper or television program themselves. Now that software is a mass medium - one that influences people's lives at both consumer and institutional levels - might not it be useful if people learned to detect software's biases?

4. HOW IS SOFTWARE SUBJECTIVE?

Example 1: Google, whose search results significantly influence the information people access, touts the objectivity of their PageRank technology:

PageRank relies on the uniquely democratic nature of the web by using its vast link structure as an indicator of an individual page's value. In essence, Google interprets a link from page A to page B as a vote, by page A, for page B. But, Google looks at more than the sheer volume of votes, or links a page receives; it also analyzes the page that casts the vote. Votes cast by pages that are themselves "important" weigh more heavily and help to make other pages "important." (Google)

I'd argue that the algorithm described isn't "democratic" but is actually rather similar to becoming popular in high school. If the popular kids like you then you can easily become popular. But what if you're not part of the in-crowd? What if you're a dissenter - or just not trendy? According to the algorithm described above, it's difficult to get noticed. Google apparently refines the PageRank algorithm on a regular basis, and they keep its exact workings a secret. (If they didn't, it's likely we'd all see even more ads than we do for products that begin with a "V" and end with an "a.") But at least we can begin to critically question how PageRank influences the information we read. And even though Google assures us that "Google's complex, automated methods make human tampering with our results extremely difficult," (Google) we can keep in mind that humans determined the automated methods in the first place.

Example 2: The United States Internal Revenue Service was recently criticized for freezing the tax refunds of many poor taxpayers by targeting their returns as likely to be fraudulent - even though most were not. An article in *The New York Times* reported that "a computer program selected the returns as part of the questionable refund program run by the criminal investigation division of the Internal Revenue Service." (New York Times)

The article doesn't tell us any more than that about the computer program, but obviously someone programmed it with rules for finding a "questionable" return. Clearly, those rules were subjective, and they seem suspiciously like they may have been politically motivated. The fact that the deed itself was done by computer doesn't make the decision mechanical, blind or objective. In a software-literate culture, the journalist who wrote the article might be expected to press for details on how the program worked, or at least discuss his inability to obtain this information from his sources. But at present, it seems largely

culturally acceptable to shrug such things off: "The computer did it."

5. I'M NOT MYSELF TODAY...

If we say someone "matches" a terrorist (or anything else) - what does it really mean? Some characteristics of that person's face have been determined to be significant - they match the terrorist face more closely than others in the database. This raises the question - what are these "significant" characteristics?

For example, in "Face Recognition Using Eigenfaces" (accessible online at <http://www.cs.princeton.edu/~cdecoro/eigenfaces/>) images document the results of an attempt to use computer vision algorithms to match photographs of individuals with those in a database. In the second photo from the top of the web page, we see that the algorithm detected the correct person from the database in a large percentage of cases (DeCoro). However, the few incorrect cases are interesting. The software attempted to detect similarity between photographs and faces - and it did so - according to *some* characteristics. Not the ones that would have given the "right" answer and identified the same person. But the wrong answers may not be what we expected - or feared. Instead of confusing people of the same race, for example, the software will sometimes confuse two people with a smug expression on their face. Maybe in some ways smug people have more in common than people of the same race. Maybe, on days when you're not yourself, you're really more like someone else. In any case, attitude profiling may turn out to be a greater risk of technology than racial profiling.

But profiling concerns aren't limited to race. If the computer vision bogeyman were used to identify "undesirables," what would those undesirables look like? Presumably, everyone could envision their own profile of an "undesirable." And in fact, such profiling could be programmed into a computer vision system. But - the profiles would need to be quantified for the computer. It turns out, computers are subject to the same type of stereotyping as humans are - only more so. For example, say you're on the lookout for troublemaking emo kids. You could tell a human, "Watch out for emo kids," and this would be asking the human to stereotype. But you'd have to tell the software, "Detect people wearing all black, with pale skin and very black hair." This is more extreme stereotyping than the human might do, at least consciously. But of course, humans chose those characteristics.

So - one of SVEN's aims is to reflect on the human subjectivity inherent in technology. Because this subjectivity must be reduced to objective rules, such implementations obviously have limitations in mimicking the way humans would perform the intended task. However, the implementations and their results can, through these limitations and exaggerations, reveal less obvious things about how their human creators "see" things - and about humans in general. Technological development expects machines to think like humans and humans to think like machines - under this stress both give something about themselves away.

6. TECHNOLOGY AND THE WAY IT'S USED AREN'T THE SAME THING.

This might seem an obvious point, but the opportunities it presents for tactical software might easily be overlooked. Take for example, computer vision surveillance technology. It conjures up depressing connotations, and our gut reaction is to respond to it by resisting. That's because we're used to it being used to find when someone looks, in someone else's judgment, well... bad.... But that's not necessarily the case. Why limit ourselves to defensive positions against "scary" technologies? Why not take some offensive ones? If computer vision can determine when we look bad, we can develop some computer vision technology that can figure out when we look good. And who looks better than... rock stars?

7. REFERENCES

[1] WikiWikiWeb Contributors. "Hermetically Sealed Stuff is Magic." WikiWikiWeb. 25 January 2003. Retrieved 6 June 2006 <<http://c2.com/cgi/wiki?HermeticallySealedStuffIsMagic>>

[2] "Our Search: Google Technology." Google. Retrieved 6 June 2006. <<http://www.google.com/technology/index.html>>

[3] Johnston, David Cay. "I.R.S. Limited Tax Refunds of Poor, Congress Is Told," The New York Times. 10 January 2006. The New York Times Company. Retrieved 6 June 2006 <<http://www.nytimes.com/2006/01/10/business/10cnd-tax.html?ei=5090&en=63292ea6712adf26&ex=1294549200&adxnnl=1&partner=rssuserland>>

[4] DeCoro, Christopher. "Face Recognition using Eigenfaces." 2004. Retrieved 6 June 2006 <http://www.cs.princeton.edu/~cdecoro/eigenfaces/>

7.1 Other relevant works:

Other video surveillance-related tactical media projects:

The Surveillance Camera Players

<http://www.notbored.org/the-scp.html>

The Tactical Ice Cream Unit

[http://www.tacticalmagic.org/CTM/project pages/TICU.htm](http://www.tacticalmagic.org/CTM/project%20pages/TICU.htm)

Other projects dealing with software subjectivity:

Reamweaver

<http://reamweaver.com>

Sinister Social Network

<http://sinister-network.com>

Other computer vision research that looks at human desirability:

Automatic Prediction of Human Attractiveness

http://www.eecs.berkeley.edu/~ryanw/research/tr_hot.html

Another text about software subjectivity:

Software Art and Political Implications in Algorithms

<http://art.runme.org/1107805961-9560-0/gonzalez.pdf>

A text from 1987 about the then-new Macintosh as a black box:

The Macintosh Computer – Archetypal Capitalist Machine?

<http://www.williambowles.info/sa/maccrit.html>

More software art and theory than you can shake a stick at:

Runme.org

<http://runme.org>