**The Lights are On and They are Watching You**

**By Nora Bauer**

(ViSmedia Conference, Bergen University Aula, March 26 2019)

Ladies and Gentlemen,

first I would like to thank Astrid Gynnild for inviting me to this years ViSmedia conference. It's a great honour.

Some time ago, in February 2014, a New York Times article caught my attention. It talked about light fixtures installed at Newark Liberty International Airport: Visitors to the terminals might have noticed the bright clean lighting that blanketed the cavernous interior, in courtesy of 171 recently installed LED fixtures. What they probably would not have realized that the fixtures were a backbone of a system that was watching them, so the article stated.

This is the topic of my today's lecture: The lights are on, and they are watching you.

There is no more common and unsuspicious looking public furniture then a street light. Just count them as you walk to your local grocery store, at least every forty steps there is one. Worldwide installed are about 4 billion.

After I read the Times-article I stepped out of the house and focused the street lights suspiciously. It is one thing to participate in social media, but quite another, to be registered as soon as I leave the house and walk down the street.

But everything looked completely innocent and quite normal to me.

In Germany it is – still, I might say – illegal to generate personal data in public areas.

The next unnerving event happened in my home town Köln.

To understand my anxiety I have to tell you something about Köln, it’s a city with about 1 million inhabitants, deeply conservative, deeply catholic and also deeply concerned about only one thing: the annual carnival – the cologne carnival is even a idiom in my English dictionary. Rumour has it, that the average colognian is born with a red nose. This might tell you something about their state of mind. They will not ever protest against public surveillance, even if they do notice it, they just don’t care. So when in 2014 I came across a sign spread across a small two-way-city-street that read: You are now entering the first Cologne-smart-street, I felt somewhat alarmed.

From then on, the headlines kept dropping. Berlin, Hamburg, Munich, Dresden, Leipzig, Düsseldorf, and even smaller places like Trier, were participating in a project called 'smart city'.

As I later found out, the main interest that hides behind this label is the installment of a certain type of light-fixtures in public areas and places: LED. They are similar to the light fixtures that were set up at the airport in Newark and are according to the New York Times-article outfitted with special chips and connected to sensors and one another over a wireless network that collects and feeds data into software: time of day, temperature, CO2-level, volume of traffic, free parking spaces, even license-plates.

Could this really be true??

I then decided to do some research on this subject and write a radio-documentary on 'the lights that can watch you'. It took three years of constant rattle until I finally found an editor at Deutschlandfunk, who took the subject seriously. Over the next months I talked to light-fixture-manufacturers, public administrators, energy-providers, sociologists, hackers, mobile service and internet providers, data processors, data traders.

I came to the conclusion that it might be illegal in Germany to draw personal data in public areas, but that doesn't mean that people who want it, won't get it. The procedure just looks a little different than using a broad open camera.

And this is what I found out:

Systems like the one at Newarks International Airport are originally invented and developed by a company called Sensity Systems, based in California. CEO Hugh Martin beforehand was head of construction with Apple.

He stated that Sensity actually started out as a LED-lighting company. But soon enough the observation was made, that there are four billion Outside-HID-Lights – High-Intensity-discharge-lights – worldwide set up, a great number of them at airports. During the next fifteen or twenty years, all of those lights would be converted to LED, because administrators will save 70% of the energy right of the top. Also instead of burning out every two years, like current HID-lights do, they last ten years and longer.

But the most important observation was, the new LEDs run of direct current just like laptops do. And just like a laptop you need a power adapter. So that actually means that there will be four billion DC power supplies twenty or thirty feet up in the air, and the labor to do that is already paid for by the streetlight. So the question for Hugh Martin really was: if you install four billion DC power supplies – practically laptops – twenty feet up in the air, what else can you do with it? And his answer was: you can build an amazing network on top of that.

Every really important network in the history of technology has been set up on top of some kind of already existing infrastructure, for example the telegraph and then telephone were set up on railroads. These four billion street lights are the existing infrastructure and can easily function as a platform, just sitting there waiting for a network to be built on top. Hugh Martin wondered what you could do with a network like that. And here I quote:

*The answer is you can generate information about the environment around the light. You gather sensory information about what’s going on around the light and make it available.*End quote.

The next person I talked to was an administrator of the Cologne Power Provider. He was absolutely thrilled with the gee-whiz technology in his smart-street, this small two-way city street I told you about. He did not have any qualms about maybe gathering compromised data at all. He stated, and I quote:

*The streetlights here were all changed into LED. We installed sensors for open parking spots, we generate data on carbon monoxide, carbon dioxide, fine dust particles, groundlevel ozone, sound level, a whole lot of other different data, that we generate here.* End quote

As Hugh Martin explained, a sensor can be anything, it can read temperature and other ecological information, but most importantly it can substitute video. It can tell, when there is a parking slot available or not. It can read the activity of smart phones in the immediate area of the light. It can generate the information about what smart phones are doing and how people are moving around in the area. That’s all available with no extra costs. Authorities can keep track of what kind of cars there are, what kind of movement is going on, the behavior of cars, how long do they stop, as well as the movement of people in an out of the area.

Since 2014, when I first stumbled across the smart-street-sign, the city of Cologne has upgraded every downtown streetlight into LED. The installed lightfixtures are manufactured by Philips. The system used is called City Touch. The LED-fixtures are outfitted with sim cards and communicate with the Philips server. Every streetlight is also provided with GPS. The city administration uses an interface pretty much like Google, on which they can drive through the city and read out the data that is generated. All LEDs are continuously transmitting their data into the internet, into the cloud – where it is stored for further reading.

A Philips commercial on this system announces:

"In City Touch our street lighting products are united to create a complete intelligent system that offers ultimate control in lighting outdoor areas of all kinds. It turns static lighting into a dynamic, flexible organ that can respond to the ever-changing situations and happenings on streets, parks and other public areas."

As I mentioned before, in Germany the right to use video surveillance is restricted. Only shops, the public transportation system, carparks and such, being a semi-private environment, are allowed to use video surveillance for property protection only. Data storage is legal for 24 hours. Only in stressed times like the annual Christmas shopping, this period may be extended.

This type of surveillance of course is manpower intensive. Imagine you have this wall with 5000 monitors that you have to watch simultaneously. You will never be able to react to any alert in real time.

The trick would be to notice an alert just in the actual spot at the actual time when and where something happens. If you have movement- and sound-sensitive lighting installed every thirty feet, this light-fixture will announce: Hey! Somebody is shooting! And with GPS installed, you know exactly where this is taking place. That is what German city councils call smart.

In order to deliver this information, the LED-fixture has to be able to read its environment completely. They do so with sensors.

Today sensors are built in everywhere, in cars, in the vegetable shelf of your supermarket, bridges, smart phones, smoke detectors, cameras. They are extremely small, measure precisely every change in their environment and feed all the gathered data into software through the internet, with which they are connected. Through these build-in sensors an object becomes smart, intelligent, sensitive in a technical sense. Their number doubles worldwide every five years. To gather information about people and their behavior 'sensory eyes' are the most important installments. You don't have to watch monitors. They signal to the connected software. 24/7. They improve security with real-time information for immediate incident response.

What began as a way to help local governments and businesses to save energy by automatically turning lights on and off, has obviously become a setup of public surveillance: The light fixtures can spot long lines, recognize cars and even identify movements as suspicious activity, sending alerts to the police.

Of course this does not have anything to do with personal data, which means it is not knowledge about anything yet.

What could a city administration then do with it?

How can you turn these large amounts of data so conveniently publically collected into knowledge about the individual behavior, and still avoid the illegal use of video and BFR / biometric facial recognition?

The data collected — say, a particular car pulling up to a certain parking spot at the same time every day — can of course be mined and analyzed for a broad range of applications.

All the German cities that partake in the smart-city-project also partake in a deal with a data-mining-company. For most cities this is either SAP or AGT International. So I talked to Martin Klein, who at SAP is responsible for the business with city authorities, governments, police administration, and municipal utilities.

Martin Klein noticed that very often city authorities do not use data intelligently. Of course they all have their software up and running but the data they collect, they do so in separate systems. Consequently they cannot generate the same knowledge out of it, which they would by putting all the data together.

For the intelligent mining of data, SAP has created an in-memory-data base, called HANA, which through certain algorithms enables the client to check or read large amounts of data either from a certain key-point or analyze it under all kinds of different variables at any time.

This is the way to create new insights.

In order for an algorithm to give valid information about individuals you have to feed it infinite amounts of data, big data.

The focus of interest has changed. People who deal with information don't care who walks down the street, but only how many people do so every day at the same time. They are not interested in the individual, but in predicting future incidents and mass behavior and than manipulate it into a certain direction. Like buying a certain product, starting a riot or voting for a certain party or president.

The best thing that can happen to an algorithm is to match all this information that is gathered anonymously with data fed in by using apps that are made available to the frequent user of the system. For example:

It’s early in the morning. You are on your way to the airport and as you’re driving, you wish you had a cup of coffee. So you use the airport application on your phone, and you say, I’m really interested in a cup of coffee, when I get there! As you get close to the airport, the application comes up and says, what airline you’re going to? You give this information and it says, all right, great, here is the number of parking spots that are available to you. Do you have a favorite level of the garage in which you’d like to park? And it tells you where the parking spots are. All of this is happening through the smart light fixtures. The airport now knows you are there because you have agreed to consent to give your information. So the coffee-shop now knows you are coming, you have ordered what you wanted, and as you are going down into the airport itself, they know, and your coffee will be waiting for yo, as you get there.

But it is not only the airport and the coffee-shop who know, it is also the algorithm. And it never forgets.

Hugh Martin from Sensity Systems told a very interesting story:

A lot of people would think Apple’s idea for the smartphone was all about a better phone. But it wasn’t about a phone at all. It was about a platform where hundreds of thousands of millions of applications could be developed and set up, and would change people’s lives. Only one of the applications on your smartphone is really a phone! And the same condition works with smart light-fixtures, only one application on it is a light.

So again it was the idea of a platform that was most important.

Cities that buy these sensory systems have different unique uses for applications that they like to solve. If they have to build a vertical application solution for every single one of these, it probably will never happen. A platform with thousands of applications that make use of all this data that is gathered by one network, which is attached to the lighting, is extremely powerful. And that’s what is called a light-sensory-network.

Then again what else is a smart city but the internet of things and services? The entire city environment will be plastered with sensors in streetlights that collect and feed data into databases. It will be a permanently ongoing communication and interaction between the surrounding technology and the inhabitants, who then become part of the technical infrastructure of a city.

Back to my home town: The city administration of Cologne is divided into different providers: water, garbage, power, and so on, which operate profit-oriented just like private enterprises. The internet provider Netcologne belongs in part to the local power provider. So they of course partake in the big LED switch by offering free wireless local area network wherever a LED light fixture is installed, to anybody who walks along there, with his smartphone on.

They don’t just read your movements, they are offering you to partake in this information-gathering and give up your privacy freely and willingly because it is manufactured as a service to you. Nowadays they put up signs, which I personally take as a warning: free WLAN on this street!

What is the outlook on all of this?

The danger is not the collecting of personal data and being registered and seen individually, but being possibly integrated and manipulated into a reality that is read and interpreted by sensors that decide about an incident on an inhuman level.

Hugh Martin's idea is as simple as ingenious. Smart housing, smart cities, smart countries, smart rivers, smart everything! And the backbone for this worldwide network is build by the streetlights.

His company Sensity Systems, in those days still a startup, was in 2016 bought by the giant Verizon for more than 2 billion US $.

What began as an energy-saver has developed into an expanding market for lights, sensors and software capable of capturing and analyzing vast amounts of data about the habits of ordinary citizens.

Another outlook will be:

Predictive policing. It refers to the usage of mathematical, predictive analytics, and other analytical techniques in law enforcement to identify potential criminal activity.

Predictive policing methods fall into four general categories: methods for predicting crimes, methods for predicting offenders, methods for predicting perpetrators' identities, and methods for predicting victims of crime.

Predictive policing methods are not a crystal ball: they cannot foretell the future. They can only identify people and locations at increased risk of crime and they are enabled to do so by infinite data collected by sensors in public areas.

In Germany politicians are about to fashion a new police-act, which allows police to gather and storage information not only about criminals, but everybody they come in contact with, even if you just report loud music and noise in the neighborhood, they will be allowed to keep your personal data indefinitely.

One of the administrators working for the German data protection legislation laughed at my naiveté. The German Home Secretary is nowadays pushing a law for legalizing BFR in public areas. With all its consequences to detect people in these areas, who's data is already known, and can be matched. Consequently, people will lose control over the guaranteed anonymity of public places, they lose their invisibility, the freedom of walking unseen. This, he said, is a development to be definitely scared about. We will have a total coverage and detection of public places matching information with a manhunt-database.

But there is no such thing as100% accuracy.

The French philosopher Jean Baudrillard 1978 wrote about the agony of the 'real' as he called it.

It used to be that the best map was the one that the cartographer painted in such granular detail that the map and the shown territory were an exact match. Today – so Baudrillard – the abstraction does not work any longer with the model of the map. The map does not rely on a real territory or substance any longer. It rather uses different models to fashion a real with no origin. The territory is not originating the map, the map creates the territory. The simulators of today mean to match the real with their models. They do so by means of downsizing the model, converting it into data, which then can be copied indefinitely. It does not have to be sensible, just operational.

Thank you for your attention.