

The Future is Now - 9/11, CCTV, and Our Brave New World

Ursula Drees

Abstract

Movies such as *1984*, *The Truman Show*, *Starship Troopers*, or *Minority Report* are regarded as imaginations of the impossible and unthinkable. Mankind defines itself as an individualised, authentic civilisation, whose independence and freedom is steadily increasing. We will nevertheless argue that these movies describe possible future scenarios and models of life under constant and unrestricted surveillance. The result will be a uniform and standardised civilisation.

Marketing will surely embrace the “personalised advertisement” as shown in *Minority Report*, where the customers’ eyes are scanned, his identity is recognized, and his habits are loaded from a database. Today, many companies save their customers’ data, some with, some without the consent or even the knowledge of the latter. The number of the already ubiquitous CCTV cameras is increasing steadily. Especially since 9/11 and the constant fear of terrorist attacks, “changes” to individual liberty have increased tremendously. Iris scanners and face recognition technologies are widely introduced to public environments.

Still, surveillance in all its forms allegedly only provides for better security and personalised content; but we should hope that the governments and companies using these techniques will continue doing so for our good only – otherwise, *1984* will easily become a pale imitation of reality.

Key words

Identification, CCTV, cyberspace, standardisation, surveillance, virtuality, individuality, identity, authenticity, vulnerability.

1. Customer Satisfaction and Surveillance in a post-9/11 Environment

Movies such as *1984*, *The Truman Show*, *Starship Troopers*, or *Minority Report* are regarded as imaginations of the impossible and unthinkable. The future they depict seems too bleak (if not absurd) for many to accept. Mankind defines itself as an individualised, authentic civilisation, whose independence and freedom is steadily increasing. We will nevertheless argue that these movies describe possible future scenarios and models of life under constant and unrestricted surveillance. The result will be a uniform and standardised civilisation. Several actual developments will be combined to make this future outlook too soon a reality. Thus, *1984*’s “Big Brother” may easily become a pale imitation of reality.

In *Minority Report*, everybody’s irises are constantly scanned, one’s identity is recognized and a connection to a database is made. Thus, wherever you walk, you receive special offers, according to your previous buys, your size, and your likings. Furthermore, individual traffic is heavily controlled: not only are speed and destination to be pre-set, the authorities can gain full control over one’s car. The combination of biometrically based surveillance and interconnected databases provides for instant location of any individual.

This brave new world, however, is far from being a mere futuristic outlook. Millions of customers are happily willing to provide even intimate data to supermarkets and retailers. Overall, 85% of British households have provided data to at least one of the such so-called “customer loyalty schemes”. Huge amounts of personal information is now in the hands of private companies. The drugstore chain Boots has a database of 15 million card holders, and the loyalty scheme *Nectar* claims to have one of the largest email files in the UK. In the US, loyalty card details have already been used in family law cases; for example, a man’s card-tracked purchase of expensive wine was used as evidence in a divorce case to show that he could afford to pay more alimony. Ethnic profiling is another possibility: according to Katherine Albrecht from *Consumers Against Supermarket Privacy Invasion and Numbering*, the FBI reviewed the loyalty card records of the terrorists involved in the 9/11 attacks to create a profile of ethnic tastes and supermarket shopping patterns associated with terrorism.¹

Radio Frequency Identification - or RFID - is now being introduced, a form of wireless electronic tagging which can be embedded into any product. According to this technology’s pioneers, the Auto-ID Centre, the ultimate goal is to assign a unique number to every product on the planet, leading to a “physically linked world”. Everyone in the possession of such a scanning device could see what you

have bought, what you are using at home, and ultimately, who you are. This technology is not only a supply chain management tool, but it is already used for combating crime: in one *Tesco* store in Cambridge, RFID tags trigger a digital camera to take a picture of every customer who takes *Gillette Mach 3* razorblades, an article that is regularly stolen.

More and more public places are constantly monitored by CCTV cameras, which have been set up by local authorities, but increasingly by private companies, too. In London, any customer will soon be filmed for the whole time he uses public transport. The *Congestion Charge* in London, a fee to enter the city centre by car, is automatically controlled by CCTV cameras. Thus, and without public dissent, the authorities can track whose car has entered and left the city at any given time. The next step would be to enforce “correct traffic behaviour”, as wireless identification devices in conjunction with the cars’ electronics could prevent motorists from speeding or other unruly behaviour.

People can be automatically identified by various means, for example by their face or parts of it, their irises, their retinas, or the many other individual parts of our bodies, such as fingerprints, ears, the voice, the hands’ geometry, or by the way one walks. Depending on the means, all these techniques have a certain element of uncertainty, even if one does not assume that somebody wants to hide his true identity.

Since the terror attacks of 9/11, two aspects of surveillance, data storage, and data processing have changed: both the willingness of governments to use such techniques, and the willingness of the people to accept constant surveillance have rapidly increased. In the same time, due to the revolution in information technology, there are many more ways to identify, tag, and track individuals and their behaviour. The necessity to use these techniques has been recognized and is being propagated, but not as a means of surveillance, but for protecting the people by combating crime and especially terrorism.

Examples are many and diverse. EU leaders agreed to include a chip with biometrical data such as eye scans in the forthcoming passport versions. US immigration offices ask for fingerprints of foreigners from specific countries. The UK is now discussing the introduction of identity cards with biometrical data, while there was always a strong opposition against any ID cards at all. The British Home Office is deploying facial recognition systems to fight fraudulent asylum applications. In numerous airports, museums, and shopping malls, biometrical identification is already used to spot individuals or to scan for unusual behaviour.

Telecommunication provider save their customers’ data and provide the authorities with far-reaching access to both this data and live communication, while the *Echelon* programme is already scanning private emails and phone calls. More and more databases and networks are linked together. Personal data is increasingly acquired by private companies, also by the outsourcing of public services, for example the possible privatisation of the British Forensic Science Service, including the DNA crime database.

Although the US Senate blocked the *Total Information Awareness Program*, intended to be a global data-surveillance system to find signs of immediate threats, there are numerous programmes leading in the same direction. The Pentagon’s *Defense Advanced Research Projects Agency* (DARPA) – once the driving force behind the development of the Internet – is also developing a system called *Combat Zones That See*, linking identification systems with surveillance cameras to monitor a whole city, with advanced data mining being the very heart of this system of systems. Florida recently introduced the aptly-called MATrIx, short for *Multistate Anti-Terrorism Information Exchange*. With this tool, it is possible to “let authorities, for instance, instantly find the name and address of every brown-haired owner of a red Ford pickup truck in a 20-mile radius of a suspicious event”. According to James Moore (former Commissioner of the Florida Department of Law Enforcement), “the power of this technology - to take seemingly isolated bits of data and tie them together to get a clear picture in seconds - is vital to strengthening our domestic security”.

The “War against Terror” seems to be an endless struggle against an amorphous enemy who - to quote Clausewitz - changes its shape like a chameleon. We still cannot foresee what restrictions in our privacy we are ready to take, nor which restrictions will be imposed. Hannah Arendt wrote in *The Origins of Totalitarianism*: “The principle of the movement is whoever is not included is excluded, whoever is not with me is against me, so the world loses all the nuances and pluralistic aspects that have become too confusing for the masses.”² So, are you with us, or with the terrorists?

2. Visions of Humanity: The Expulsion from Paradise

Why do we accept these new levels of constant and unrestricted surveillance?

First reason. The relationship between nature and technology in today's society has profoundly changed.

Second reason. An increased standardization and conformity of humankind within society, due to a pronounced wish for acceptance.

Third reason: Creation of a second self by means of Virtual Reality

First reason. The relationship between nature and technology in today's society has profoundly changed.

"The expulsion from Paradise is not a loss; man creates a new, more blissful paradise" through his "art". (George Agricola and Paracelsus)

Nature as such exists and reproduces itself. Mankind, however, only exists due to its constant action, reproduction, and reinvention. Nature is thus acting in a paradoxical way, being spontaneous and expedient at the same time.

Modern man, however, has entirely lost his connection with nature. In principle, nature can be manufactured and reproduced by man.

For us dealing with nature means to change and improve it, making it fit our ideals. Most people not only assume that every natural product can be technically reproduced, but also that all natural processes will be simulated and replaced soon, including ourselves.

The following objectives of human progress may be derived from technological progress:

1. Increased striving for autonomy from nature.
2. Gaining more available time.
3. Increase in knowledge and abilities.
4. Decrease in work-load and improvements in the quality of life.

To summarise: man masters nature through technology. He gains freedom and independence, but at the same time loses knowledge and a natural way of relating to life.

This leads to the second reason. An increased standardization and conformity of humankind within society, due to a pronounced wish for acceptance.

Harold Innis states:

The exploitation of a particular communication technology fixes particular sensory ratios in members of society. By fixing such a relation it determines a society's world view; that is, it stipulates a characteristic way of organizing experience. It thus determines the forms of knowledge, the structure of perception, and the sensory equipment attuned to absorb reality.³

For man's social existence, rules are necessary.

They determine the manners of dealing with one another, create laws and thus also a society's morals and ethics. Without them, the highly complex Western societies would collapse. Yet where new rules and laws are effective, new norms come about that are meant to show man the right way.

Contrary to rules and laws, which tell people how not to act, norms illustrate what society regards as normal. Therefore they don't describe a way that contains what is right for every individual, but rather constitute the mean of the sum of all individual desires.

A life of anonymity, of a systematised norm, makes people feel safe and protected. It allows each individual to strive towards the standardised ideal.

Thus in the area of genetic engineering during the past few years, the use of computers has led to a progress that make it possible to significantly manipulate a person's genes. They enhance, e.g.,

1. control of the ageing process, of muscle growth or growth in general;
2. control of one's appearances through plastic surgery;
3. increase of mental capacities through chip implants;
4. the ability to combat diseases and epidemics.

These examples perfectly express the struggle towards an ideal norm and the desire for man's ultimate rule over human finiteness.

We have an identity in the physical-natural world but need an additional identity for the world determined by technology.

Which leads us to the Third reason: Creation of a second self by means of Virtual Reality

In his book *Connected Intelligence: The Arrival of the Web Society* the media philosopher Derrick de Kerckhove says: "One of the main effects of digitisation is to make 'liquid' everything that is solid. Anything that can be digitised can be translated into anything else that can be digitised."⁴

We can distinguish three levels of virtuality:

- (1) virtuality as an instrument for simulation
- (2) virtuality as a prosthesis
- (3) virtuality as a surrogate world

The first level: virtuality as an instrument for simulation

Currently virtual reality still largely serves to simulate genuine realities; it is used, e.g., for driving simulation, computer games or for medical applications. Virtual reality as an eye, as an instrument for visualisation.

Such as: Virtual interior furnishings, virtual buildings and constructions, flight simulators, computer simulation of human behaviour in psychology and brain research, etc.

The second level: virtuality as a prosthesis

VR as the extension of an arm, computers as prostheses to compute, think, observe, control, stimulate, and so forth, as means to boost and enrich the imagination.

Examples: Medical applications, such as minimally invasive diagnostics and surgery, robots, androids or humanoids (toys *Kismet* or the *Sonydog*), clone, websites, chat rooms, cybersex, etc.

The third level: virtuality as a surrogate reality

The prosthesis takes on a life of its own, the computer turns into a creation machine.

Virtual worlds replace the real world. This happens through the perfecting of simulation: avatars, mock identities in the Net; caves or holo-decks, etc. or through linguistic identification (metaphors), propaganda, e.g.: reportage on military conflicts and wars (Gulf War), advertising, news

The price to be paid for these new abilities is high:

1. Loss of historical knowledge and abilities: dried milk instead of mother's breast, crafts and repair works, no larder in modern buildings, home trainers instead of outdoor activities and manual work, etc.
2. Loss of history
3. Loss of identity and authenticity as human beings
4. Collective loss of reality.
5. Vulnerability of the information society.
6. Receiving masses of junk information and spam.
7. Loss of the experience of direct contact with nature and other human beings. De-naturalization of everyday life.
8. Having more trust in machines than in human beings.

Donald Theall on the significance of convergence in cyberspace: "Ultimately, the full development of cyberspace, or virtual reality, will provide people with the capability to interact within all-encompassing environments across space and time, while simultaneously utilizing data bases of varying media mixes from many distant and disparate locations."⁵

Human self-perception and -definition is referring to one's own personal sphere of action, not towards the public at large. Out of it, a lack of interest in societal and political problems, issues, and developments is generated.

This lack of interest is being nurtured by an uncontrollable amount of information. Due to modern media and its 24/7 flood of information, man feels well informed, enlightened, individualised, authentic - and very happy. What will be the impact of this media hybrid on human communication, and, more important, on his identity?

There are numerous and increasingly interconnected databases, set up by the authorities and by private companies alike. The diverging interests of these different actors are leading to different outcomes for the data's source - us. We will not be able to control who has which access to which amount of our personal data. It is said that "those who control the past, will control the future", but for us it is "those who control the present, will control the future".

3. Conclusion

We already live in the world of *Minority Report*. The march of history surely cannot be halted. However, we all should consider wisely whenever we happily hand over personal data to a marketing agency or a customer loyalty scheme. Security is an important issue in our times, shaped by an increasing insecurity due to globalisation, the radical change of our societies, and the international threat of terrorism. Our wish for security, however, may paradoxically lead to even more insecurity, the loss of identity, and the loss of history. The image of uber-individuality, communicated by clever marketing, is already a fake. Individuality and authenticity was yesterday - tomorrow will be the age of the adjustable

mass, in the same way that nature has become adjustable to us. We do not think any longer, we believe. It is time that machines will rise to power.

Notes

¹ <http://www.nocards.org>

² Arendt, Hannah (1979), *The Origins of Totalitarianism*. San Diego: Harcourt Brace Jovanovich, pp.380-381

³ James Carey (1969), *Harold Adams Innis and Marshall McLuhan* in Raymond Rosenthal, ed. McLuhan: Pro and Con. London: Penguin Books, p. 284.

⁴ Derrick de Kerckhove (June 1997), *Connected Intelligence: The Arrival of the Web Society*. Somerville House Books; p. 148

⁵ Donald Theall (1950), *Beyond the Word: Reconstructing Sense in the Joyce Era of Technology, Culture and Communication*. Toronto: University of Toronto Press, p. 21

Bibliography

Arendt, Hannah. *The Origins of Totalitarianism*. San Diego: Harcourt Brace Jovanovich, 1979

Carey, James. "Harold Adams Innis and Marshall McLuhan." In: Rosenthal, Raymond, ed. *McLuhan: Pro and Con*. London: Penguin Books, 1969

Hammer, Volker & Rossnagel, Alexander & Wedde, Peter. *Die Verletzlichkeit der Informationsgesellschaft*. Wiesbaden: Westdeutscher Verlag, 1990.

Johnston, Philip. "DNA crime database may be privatised." In: *Daily Telegraph*, July 18, 2003; p.7.

Jonas, Hans. *Das Prinzip der Verantwortung*. Frankfurt/Main: Insel, 1985.

Kerckhove, Derrick de. *Connected Intelligence: The Arrival of the Web Society*. Toronto: Somerville House Books, 1997.

Ropohl, Günter & Lenk, Hans. *Technik und Ethik*. Ditzingen: Reclam, 1987.

Shabi, Rachel. „The Card Up Their Sleeve.“ In: *The Guardian Weekend*, July 19, 2003; pp. 14-23.

Theall, Donald. *Beyond the Word: Reconstructing Sense in the Joyce Era of Technology, Culture and Communication*. Toronto: University of Toronto Press, 1950

About the Author

Ursula Drees is the founder of the interactive media company *plusinsight*, specialized in design technology, communications, and information-related and educational products. With more than nine years of experience in the industry, Ursula Drees has managed the integration of computer-based systems in design communications for a variety of design firms and software companies like Pixelpark GmbH, Berlin, Germany, Unified Field, Inc. New York, USA, and artemedia ag/Filmstudios Babelsberg, Germany.

Besides her professional work at *plusinsight* she is teaching *Mediaphilosophy* and *Mediadesign* at the Polytech University for Applied Sciences in Berlin. She has a Master's degree of Fine Arts of the University of Fine Arts, Berlin, Germany and a Diploma degree in Visual Communication and Design, with special emphasis on interactive media. Email: udrees@plusinsight.de