

::: www.gehennainc.com - CCortex

USE AND MISUSE OF INFORMATION: BOTH SIDES OF SURVEILLANCE

Tommaso De Benetti
info@gehennainc.com

INTRODUCTION

« *All I need now is information* »

Solid Snake in Metal Gear Solid (Hideo Kojima) / Konami KCEJ, 1998

The issue of surveillance society is, as David Lyon claims, “of sociological interest because it contributes to the very ordering of society. And thus the other face of surveillance arises from its capacity to reinforce social and economic divisions [...] Those surveillance capacities are used to sort and sift populations, to categorize and classify, to enhance the life chances of some and to retard those of others [1]”.

What is then the reason of all this surveillance? Government and companies have the right to do this, hiding behind the excuses of “security” and “efficiency”? Why and when surveillance is not only useful, but *necessary* to maintain the social order? Last but not least, where is all this information going? Where is it stored, and what will happen to it in some years from now? Can we really manage such an enormous flow of information? Let's see...

THE SHAPE OF SURVEILLANCE

Hammersly : « *Look, I'm not gonna sit in congress and pass a law that lets the government point a camera and a microphone at anything they damn well please* ».

[...]

Reynolds : « *Look, I don't care who bangs who, which cabinet officials get stoned. But this is the richest, most powerful nation on earth, and therefore the most hated, and you and I know what the average citizen does not, that we are at war twenty-four hours of everyday. [...] Do I have to itemise the number of American lives we've saved in the past twelve months alone with the judicious use of surveillance intelligence?* ».

Abstract from Enemy Of the State script by David Marconi, film directed by Tony Scott, with Will Smith, Gene Hackman and others / Touchstone Pictures, 1998

Some surveillance practices have been a feature of modern life for a long time. Medical records, voting lists, housing registries, tax files and employee numbers are part of what everyday living is all about, at least in urban industrial societies...Indeed, they facilitate modern life by giving evidence of eligibility and entitlement to benefits and privileges, even though they simultaneously place power in the hands of the system processing the information [2]. In the past days, surveillance was a process in which embodied persons were watched by others. Nowadays the situation is changing: surveillance practices and flows of data move almost without limits between one sector and another. That's a real problem, as we will see further on, specially when we can't know for sure who is going to access to all the collected data and there's no guarantee that anybody is going to merge different databases in order to obtain our complete profiles..

As Lyon argues "the mobility that characterizes the present, itself representing a merger of speed, light and power. Nomadic bodies and digital personae are the subjects of contemporary computer-based surveillance, and are categories altogether more slippery and malleable than those utilized in previous surveillances regimes. Indeed, nomadic bodies, digital personae and relationship between them are themselves constituted by surveillance practices, which is a further sense in which interactivity occurs. Note also that while bodies still occupy space, digital personae do not, but contemporary surveillance deals in both currencies at once, and interchangeably" [3].

We can find examples of surveillance everywhere, in daily life as well as in particular situations and we don't need to be criminals or special subjects to be traced. Instead, the "common man" is probably a more interesting issue for government and, of course, commercial companies.

In urban daily life myriad of checks are made to ensure that we are in the right place at the right time, travelling at the right speed or carrying the correct items. We are positioned, placed, directed, and traced as we travel, buy, study, telephone, find entertainment and work [4]. Cameras are everywhere, into public transport vehicles, buildings, elevators, tubes, shops. GSM mobiles always send signals at regular intervals even when they are

turned off (the only way to stop the data exchange is to remove the battery). UMTS mobiles allow other people to see where you are and what you are doing every time you answer a call. GPRS integrated function (in cars/mobiles/handhelds...) can locate you with an excellent approximation.

Where all this devices/features have been installed, citizens seem to take them for granted. This without considering biometric surveillance that is also spreading very fast. According to Davis, in 1997 there were already over 10.000 locations in the USA, from bank vaults to blood banks, where one had to present a body part to go through a door or gain access to a file [5]. As Poster claims, "subjects constantly participate in their own surveillance by making cell phone calls, automated bank transactions, internet booking and so on" [6]. Related to this topic, is impressive the report of the American Civil Liberties Union about credit card transaction. People who make loans want to make sure they will be repaid, and that means keeping track of information such as the following:

1. Identifying information: name and spouse's name, social security number, address, and telephone number;
2. Financial status: amount of income (present and past), employer (present and past), occupation, sources of income;
3. Credit history: previous types, extent, and sources of credit granted
4. Existing line of credit: payment habits, outstanding obligations and debts, extent of current lines of credit;
5. Public record information: lawsuits, judgments, tax liens, bankruptcies, arrests and convictions;
6. Prior requesters: names of subscribers who requested information on the individual in the past [7].

While trying to explain the reasons of this (excess of) surveillance, Frank Webster featured several issues. "We must *know about people* if we are to arrange social life: what they buy, and when and where; how much energy they require, where and at what times; how many people there are in a given area, of what gender, age and state of health; what tastes, lifestyles and spending capacities given sectors of the population enjoy. Bluntly, *routine*

surveillance is a prerequisite of effective social organization" [8]. And, after all, "it is undeniable that individuation requires that people be monitored and observed [...] [to] being sure of receiving entitlements without which they may be limited in their capacity to be true to themselves [9]. Another (not secondary) issue involve, of course, social/national security.

The point is that surveillance, once restricted to the administration of bounded territories, is steadily experiencing globalization and virtualization along with the diminishing power of the state. Nowadays the state has no needs to hold onto full powers of surveillance when social ordering is achieved by many other agencies that have their own highly effective surveillance practices. [10]

Then, a new kind of Bentham panoptic vision is rising among us: we are watched 24/7 and, incredibly, we are (in most cases) happy about it. But surveillance has a dark side too, and carries with it numerous dangers... for example: are the effects of surveillance positive for everybody?

DANGERS RELATED TO SURVEILLANCE

As we said early, there are at least two related issues to worry about speaking of surveillance. The first one is the fear that agencies may have access to files collected for other purposes; the second one concerns the possibility of melding disparate databases.

Already in 1977, the U.S. Privacy protection Study Commission warned that "The real danger is the gradual erosion of individual liberties through the automation, integration, and interconnection of many small separate record-keeping systems, each of which alone may seem innocuous, even benevolent, and wholly justifiable" [11].

Coming back to the common and "well know" urban reality, when someone buys some groceries at the supermarket, the information needed to process the credit card transaction is not the only information that passes through the check stand. Anyone who belongs to a popular supermarket "discount club" creates a record of every item purchased, combining the information scanned from the items at the register with the person's identifying information in the

store's computer. The supermarket can use this information for any purpose. This same process can occur at any time a consumer fills out a product registration or warranty card.

In *Minority Report* (film directed by Steven Spielberg, based on a novel of Philip K. Dick, with Tom Cruise, Colin Farrell, Max Von Sydow and others / 20th Century Fox – Dreamworks, 2002) advertisements along the street were able to analyse and recognize people suggesting them what they needed: a new pair of trousers, new contacts lenses, a bigger car and so on.

Of course, internet amplifies the problem: several websites store cookies, files filled with users' preferences. Cookies are useful for users too, but on the other hand the information can also be used to generate personalized spam or it can be sold to other marketers (creating more spam).

As Lyon claims "the more people are categorized and classified by surveillance systems, the more they are sorted and split up into segments of the population, with whom they have some traits in common. [12]". This is particularly relevant if we consider the problem of discrimination against not-secure subjects. Let's think at the insurance companies. Surveillance is significant here because it is the means of determining risk and so, indirectly, of profoundly affecting life chances [13]. Even worse is the prospect of full surveillance before being hired by someone. The employee is, even now, deeply checked using special databases or genetic screening, to prevent any possible problem on the workplace and to determine susceptibility to disease. Easy to imagine that this kind of surveillance is strictly connected with the danger of inequity.

In health care, policing and the workplace, DNA data is increasingly sought. As a weapon in the struggle with disease, for example, it is believed to hold tremendous power of prediction and prevention. But the same techniques may also be used with less positive outcomes [13].

Gattaca (film directed and written by Andrew Niccol, with Ethan Hawke, Uma Thurman, Jude Law, Gore Vidal and others / Columbia Tristar Picture, 1997) gives us a warning about this kind of surveillance. The sci-fi plot tells about a strictly monitored society where people are discriminated by genes instead of

gender, race or religion, and where families, to assure the progenies to the elite, can "order" a customized "super-baby".

Using the words of Roger Burrows, "the new apartheid becomes very much a technological matter as the homeless and poor are channelled away from the air conditioned virtual environments of the great middle mass of the population."

Coming back to the danger of melding databases: several discourses raised about surveillance turning into simulation. As Mark Poster argues, computer databases may construct "subjects" or, rather "objects", whose identities are dispersed [15]. Simulation's seductive claim is that "any image is observable, that any event is programmable, and thus, in a sense, foreseeable" [16].

But what are the consequences of such simulation? What's the difference between working with mathematical models and empiric data? What kind of tricks will we face? There are no answers now, because this is the big challenge of surveillance in the next future; but we can already try, even with the help of futurologists and science fiction "warning", to avoid at least the bigger mistakes.

ACCUMULATION OF INFORMATION: COLLAPSE OF THE STRUCTURE

Colonel : « *But in the current, digitized world, trivial information is accumulating every second, preserved in all its triteness. Never fading, always accessible.* »

Rose : « *Rumours about petty issues, misinterpretations, slander...* »

Colonel : « *All this junk data preserved in an unfiltered state, growing at an alarming rate.* »

Rose : « *It will only slow down social progress, reduce the rate of evolution.* »

Colonel : « *Raiden, you seem to think that our plan is one of censorship.* »

Raiden : « *Are you telling me it's not!?* »

Rose : « *You're being silly! What we propose to do is not to control content, but to create context.* »

[...]

Rose : « *Not even natural selection can take place here. The world is being engulfed in "truth."* »

Colonel : « *And this is the way the world ends. Not with a bang, but a whimper.* »

Rose : « *We're trying to stop that from happening.* »

Colonel : « *It's our responsibility as rulers. Just as in genetics, unnecessary information and memory must be filtered out to stimulate the evolution of the species.* »

Surveillance simulation implies another critical problem: the immense amount of data. As Bogard says, it is "the fantastic dream of seeing everything capable of being seen, recording every fact capable of being recorded, and accomplishing these things, whenever and wherever possible, prior to the event itself" [17]. But this "dream of perfect knowledge" is really achievable? Are there companies/agencies capable to have complete knowledge over people and environment using mainframes? Such absolute power is difficult to imagine. The sheer mass of data would be impossible to handle.

That bring us into another issue: what happen to all this information? The progressive accumulation of data simply can't continue forever. Databases are more or less eternal, easy to copy or transfer, and can store any kind of information (text, images, videos and so on). "Something wicked this way comes" says the proverb, and the probability of structure collapse is definitely high. Computer viruses and spam e-mail may cause the internet to collapse in the near future. On this topic Hannu H. Kari, a Finnish researcher, professor at the Helsinki University of Technology claimed that internet will collapse in 2006, looking at the current trend.

Intel, Cisco, At&T and Hewlett-Packard seem to be of the same opinion: the end of the world wide web is on the way, cause millions of new computer users from developing nations are coming. The infrastructure simply can't handle them all [19].

The organised global network will function less and less smoothly, becoming progressively more prone to manipulation. The result will be that the volume of spam in the network passes the pain limit and undermines the credibility of information gathered from the internet. Even now, without waiting for the collapse, gathering the information that you need on the internet is an hard job. Too many useless information, spam, rumours, wrong reports, unverified sources. Nowadays truth doesn't exist anymore, on the world wide web. You just have to believe in the one you like more, or you find more credible.

Is this a crucial issue for governments? Should they "create context" and "filter" information, as said in the quote at the beginning of this paragraph?

In my opinion I think that, yes, governments should do something about this problem, but we have to consider that there's no much difference between this and censorship. Esther Dyson, in *Cyberspace And American Dream* [20], talks about a "Third Wave Governments", featuring five characteristics about this "new kind of government". I guess that finding a way to solve this key problem (maybe with a bilateral work involving both governments and users associations) is vital for the future of our society, and for "Third Wave Governments" too.

CONCLUSION

Surveillance is driving us through the path of efficiency/evolution/security? In some undeniable ways, yes. But when I read things like this: "[Internet 2.0] A big part of the promise is that it will turn the Web around: instead of having to find information or entertainment, it will find you — and be exactly what you want or need at that moment. The network becomes a butler [21]", I realize that the "panopticon world" described in *Minority Report* is really upon us. Then, the (maybe) ingenuous suggestion of Esther Dyson ("Our best defence [against government spying] is offence. Spy back! We need the ability to follow more closely what governments are doing") sounds good to me. When I think at the future of information, I see a world were more conscious citizens are happy for all the advantages of surveillance, but still aware of what is right and what is dangerously crossing the limit.

Notes

[1] *Surveillance Society – Monitoring everyday life* (David Lyon) / Open University Press, 2001, pag.4

[2] *Ibidem*, pag.142

[3] *Ibidem*, pag.35

[4] *Ibidem*, pag.50

[5] Cited in *Surveillance Society – Monitoring everyday life* (David Lyon) / Open University Press. No specific source.

[6] *The Second Media Age*, (M. Poster) / Cambridge Polity Press, 1997

- [7] *Your Right To Privacy* (American Civil Liberties Union) / Carbondale, Southern Illinois University Press, 1990, pag.119
- [8] *Theories Of The Information Society – 2nd Edition* (Frank Webster) / Routledge, 2002, pag.205
- [9] *Ibidem*, pag.207
- [10] *Surveillance Society – Monitoring everyday life* (David Lyon) / Open University Press, 2001, pag.30
- [11] Cited in *Privacy In The Information Age* (Harry Henderson) / Facts On File, 1999, pag.19
- [12] *Surveillance Society – Monitoring everyday life* (David Lyon) / Open University Press, 2001, pag.66
- [13] *Ibidem*, pag.46
- [14] *Ibidem*, pag.69
- [15] *Ibidem*, pag.108
- [16] *The simulation of Surveillance: Hypercontrol in telematic societies* (W. Bogard) / Cambridge University Press, Cambridge, 1996, pag.68)
- [17] *Ibidem*, pag.4-5
- [18] http://www.unspam.com/fight_spam/articles/1463.html
- [19] http://www.forbes.com/execpicks/feeds/general/2004/09/10/generalcomtex_2004_09_10_ir_0000-5884-KEYWORD.Missing.html
- [20] *Cyberspace and the American Dream* (Esther Dyson), from *The Information Society* / 1996
- [21] http://www.usatoday.com/tech/webguide/internetlife/2004-10-01-cover-web_x.htm
- [22] Cited in *Privacy In The Information Age* (Harry Henderson) / Facts On File, 1999

