The fateful click: Soft surveillance in today's control society

Reingard Nethersole

What could be more persuasive in our everyday digital high-tech world than the imperatives "google!" and (in Facebook-speak) "friend!"? Who would suspect these two hortatory commands that on the one hand urge us to look for information online, and on the other to join the 800 million active users of the social networking site Facebook[1], of opening the arena of ever more encompassing global surveillance? How can it be that an innocuous mouse click makes me part of the act of observing while simultaneously allowing for the condition of being observed? After all, neither my personal Internet search for knowledge nor the reassurance with which "Facebook helps you connect and share with the people in your life", as the site asserts, seem to have anything to do with the proverbial, more sinister Orwellian Big Brother "hard" surveillance with CCTV cameras, nowadays surreptitiously installed in shops and on buildings along city streets and public squares.

Yet from the same "hypertechnology"[2] derives what I call "soft surveillance", that is data in digitised form collected from increasingly mobile computerised devices in homes and cars for the benefit of free-market commerce, in contrast to "hard surveillance" that in the name of the state electronically assembles and sifts data ostensibly for the purpose of protecting communities and keeping the population secure. That is to say the invention of the microchip in the sixties and subsequent innovations by the information industry made possible machinic data collection on an unprecedented scale in respect of both "hard" surveillance, encompassed in Bentham's Panopticon, and "soft" surveillance incorporated in the architecture of, for instance, Google's and Facebook's digital platforms. When even the briefest connection to the Internet leaves a footprint on gigantic servers, at stake are not so much the ethics of surveillance evoked in judicial

[1] All references to Facebook can be checked with the relevant Wikipedia entry that provides a comprehensive overview of the workings of this particular social networking site, and subject of a much celebrated 2010 Hollywood movie.

[2] This is the term with which the French philosopher of technology, Bernard Stiegler, signals the current evolution of *technics* from the time of the inception of hand-held tools to machinic production and reproduction in the industrial age (technology) and finally to digitisation ("hypertechnology") in our time: *Technics and time 1. The fault of Epimetheus*, Richard Beardsworth and George Collins, trans. (Stanford: Stanford University Press, 1998).

© *African Yearbook of Rhetoric* 3, 1, 2012, ISSN 2220-2188:
Reingard Nethersole, "The fateful click", pp. 89 - 98.

considerations concerning rights to privacy; the focus rather needs to fall on the fundamental shift in the production and storage of data and with it not only changing mnemotechnologies of data retention but its control.

Inconspicuous, small additions to the lexicon and word usage, arising from networked interaction like “to google”, “facebooking”, “tweeting” and “to friend”, indicate current changes in the social milieu. Originally a proprietary name for the well known search engine, the venerable OED (*Oxford English Dictionary)* included and thus consecrated the usage of “google” as a verb in 1999. According to the *Seattle Times* (4 July, 2005)[3], the use of Facebook had already become so ubiquitous that the generic verb "facebooking" was coined to describe the process of browsing others’ profiles online or updating one’s own. Similarly, “to tweet” or “to send a tweet”, meaning to communicate with the briefest of message testify to the omnipresence of a wireless universe. Not to mention the newly coined “to friend” (a compound of the noun “friend” and the verb “befriend”) and its opposite corollary “I *un*-friend you”, that circulate prominently in the discourse of the users of a fast increasing and expanding Social Media network such as, among others, Facebook, My Space, Twitter, YouTube, and the professional site LinkedIn.

It is these digital platforms together with internet usage in general that configure the contact zones in which, largely unbeknown to their users, the postmodern “societies of control” operate hard on the heels of the Bentham-Foucault (modern) Panopticon that set the template for “disciplinary societies”. According to Deleuze:

> …the *societies of control*, are in the process of replacing disciplinary societies. ‘Control’ is the name Burroughs proposes as a term for the new monster, one that Foucault recognizes as our immediate future.[4]

Whereas the relatively closed system of the modern (nation-) state kept its citizen-subjects compliant with its rules and regulations by instilling in them “discipline” largely on the model of “hard” surveillance, epitomised in the spatial arrangements of its public institutions like prisons, schools, barracks, hospitals, and such like, the postmodern state in its commingling of digital technologies, economic interest and population welfare is increasingly capable of utilising “soft” surveillance, or in Deleuze’s terms “ultrarapid forms of free-floating control”[5]. Such “control” in purportedly open, democratic societies, is welcomed by neo-liberal “flat world” enthusiast*, New York Times* journalist, Thomas Friedman, who oblivious to its consequences readily embraces it because thanks to digitisation:

[3] See: http://community.seattletimes.nwsource.com/archive/?date=20050704&slug =btfacebook04 : accessed 11 Nov. 2011.

[4] Gilles Deleuze, “Postscript on the societies of control”, in *October* 59 (1992): 3-7 [3].

[5] *Ibid.*

> …everything can be shaped, manipulated, and transmitted over computers, the Internet, satellites, or fiber-optic cable.[6]

Friedman hails as innovative and decisive for the twenty-first century the fact that "social and business interactions" are increasingly becoming "virtual", "mobile" and "personal". "Virtual" refers to the transmission of digitized content that can be done with:

> …total ease, so that you never have to think about it – thanks to all the underlying digital pipes, protocols, and standards that have now been installed. 'Mobile' means that thanks to wireless technology, all this can be done from anywhere, with anyone, through any device, and can be taken anywhere. And 'personal', means that it can be done by you, just for you, on your own device.[7]

enabling much touted 24/7 global connectivity.

What could be more enticing for me than to have easy access to information from remote locations, to share my message with the world, enhance learning and to shape, manipulate and transmit my own "Profile" and "Timeline", as Facebook would have it? Have I not in this "flat", Brave New World left far behind the scenes staged in the fictional realm by George Orwell in his 1949 dystopian novel *Nineteen Eighty Four*, and in the realm of *Real*-politics by, among others, the infamous KGB and *Stasi* (the former East German state security system)? Although coercion by the state has been replaced by invitation to join in the circulation of goods and services in a Free Market society, "soft" surveillance is operative every time I complete a survey, take part in a poll, and login. Especially when I log into my "virtual", "mobile" and "personal" devices like a laptop, cell phone, iPad, or GPS my data — however infinitesimal — is collected, collated, connected, and my path through life dutifully tracked, logged and archived, to an extent that remains by-and-large veiled to me, the *citizen-subject*. To be sure, as *subject-consumer* I might find my demand met and my desire instantly gratified by a novel product or improved service, uniquely tailored to my apparent wants; polling and tracking my current opinion and feelings about a political candidate might affect debates in parliament, but where, how, and by whom my data is utilised and controlled remains utterly opaque.

The trick in surveillance and observation, the secret of the Panopticon is, as Jeremy Bentham pointed out, to hide the surveillance from the

[6] Thomas Friedman, *The world is flat* (New York: Picador; Farrar, Strauss and Giroux, 2007): 187.

[7] *Ibid.*

prisoners or, in Foucault's "disciplinary societies" to internalise certain techniques of subjectivation in conjunction with "governmentality",[8] that is the power of the state, characterised by growing bureaucratisation in the modern period And it is the vast amount of personal information that companies like Google and Facebook collect to run their businesses that is increasingly becoming too valuable for police and governments to ignore. Despite such companies trying to keep their users' information secret, their business models depend on exploiting the trace I leave with a mouse-click and its attendant information to sell targeted advertising. Due to my consent to use the Internet company's software I consent to the transfer of every snippet of data, every online profile I built, including the unlimited "processing" of said data by nobody in particular. That is to say because I can have their service at no cost, Facebook, Google and Microsoft can, in return, surreptitiously extract from me and all their other "visitors" information for the purpose of attracting influential advertising leaders. And when governments demand they hand it over, they have little choice but to comply. Not only are Internet companies such as Google, Twitter and Facebook increasingly co-opted for surveillance work as the information they gather proves irresistible to law enforcement agencies — it is plenty and comes with a very low cost quotient — but spying on social media users by more oppressive governments for the purpose of detecting dissident thought is common from China to North Africa. And right now, even the US Congress is debating a law that would give the courts power to censor the world's Internet by forcing service providers and search engines to block any website on suspicion of violating copyright or trademark legislation, or even failing to sufficiently police their users' activities.

Thus the three defining elements of surveillance: *distance* (between observer and observed), *concealment* (the surveilled does not know her surveillant and is not given a platform to respond), and witting or unwitting *compliance* with the surveillance operations, are the same in both "hard" and "soft" surveillance. However, the latter rather exacerbates the situation in two ways. At first, "soft" surveillance exponentially extends *distance* via technologies of Cloud Computing that provide computation, data access and

[8] Michel Foucault, "Security, territory, population", in *Lectures at the College de France 1977-1978*, Michel Senellart, ed., Graham Burchell, trans. (Basingstoke and New York: Palgrave Macmillan, 2007): 108-109, 115-16; this term appears in Foucault's later work and marks the entry of the question of the State into the field of analysis previously devoted to the study of the disciplines and biopolitics. Three things are to be understood by this neologism: the transfer, alienation, or repression of individual wills; the state apparatus (*appareil d'Etat)* set up in the eighteenth century; and finally a "general technique of the government of men" that was "the other side of the juridical and political structures of representation and the condition of the functioning and effectiveness of these apparatuses" (*ibid.* 386).

storage services, no longer requiring end-user knowledge of the physical location and configuration of the system which delivers their service. Secondly, in so far as digitised automation of surveillance and threat detection operate with the same software, "soft" surveillance ultimately utilises the same *concealed* technical control of algorithms to create specific ambient awareness in all societal milieus.

Sociologists call "ambient awareness" a specific filtering of a large number of minute pieces of informal and mundane snippets of information which as substantial part of the everyday environment our minds are processing even though we do not notice it. Yet, despite us not being consciously aware about what is going on around us we make significant judgments on the basis of this stream of small pieces of information. Corporations, state agencies, the media, social networks, in short every purveyor of web-based collaboration tools and social project management "shapes, manipulates and transmits", in Friedman's term above, context specific ambient awareness with which to combat increasing information overload. Businesses because of the broad set of information provided by ambient awareness to their teams of workers embrace it because it helps to make work visible to assure cooperation and efficiency. Recourse to Facebook, Twitter, and YouTube can create a closer digital/ambient, albeit *concealed,* bond not only between producers and consumers so as to tighten the gap between them in all areas of commerce by way of imaginative, ambient marketing, but the state can intersect with everyone and constantly update the information flows on the population ostensibly to assure its health and protection. Oversight, it will be recalled, became a fundamental tool in the Panopticon, its guard attempted like Big Brother to make visible only to himself every aspect of the inmate's life; today digitised ambient awareness enhances the tools of oversight making possible an all pervasive "soft" surveillance under diffused powers. Increasingly the question becomes one of who filters information, who holds the power of the algorithm and who controls its access by way of prohibition and regulation, given the (postmodern) filiations between hypertechnology, the supposedly self-regulating Free Market and the state.

In as far as "governmentality", the multiple interplay of "sovereignty and disciplines, as well as security", ("the state", the "bodies of individuals", and "populations")[9] has been rendered more complex due to the digitisation of all spheres of life, it is becoming more difficult to separate the domains of market and state, and consequently the question of who overseas whom. Particularly in consensual democracies like the United States, utterly focused

[9] Foucault, *Lectures at the College de France,* 12; and see Foucault's statement: "...sovereignty is exercised within the borders of a territory, discipline is exercised on the bodies of individuals, and security is exercised over a whole population" (*ibid.* 11).

on *homo economicus* and under the sway of what Deleuze referred to once as "the *cogito* of the Marketplace",[10] control of information and with it the immense archive built-up in search engines inevitably turns into a battle ground between economic rationality with its attendant self-interested *subject-consumers* on one side and on another the legislative need to uphold the state's compact between itself and its *citizen-subjects.* (Demonstrated by the tussle between trademark legislation and citizens' right to free speech mentioned above). For Foucault, the form of governmentality based on an "American neo-liberal conception" that turns first on "the theory of human capital" and secondly on "criminality and delinquency",[11] makes disputes "between individuals and government look like the problems of freedoms" in contrast to France where they "turn on the problem of public service".[12] However, in both cases biopolitics of demographic distribution together with management and control over life suggest that "the general economy of power in our societies is becoming a domain of security" or is "at any rate dominated by, the technology of security".[13] That means ubiquitous surveillance.

However, the state of affairs mapped by Foucault remains hidden under both the ease and speed with which my mouse click transports me into an Online world of unlimited possibilities, a scene of countless activities replete with the rhetorical device of diatyposis, recommending to share [someone else's] "goals of promoting the value of innovation to our economy while giving people the power to share and make the world more open" (Facebook). More importantly, the Internet replicates and even enhances a social milieu dominated by Skinnerean behaviourism that operates, to use Foucault's words, through "mechanisms of reinforcement, a given play of stimuli" entailing responses "whose systematic nature can be observed and on the basis of which other variables of behaviour can be introduced".[14] Put differently, in so far as to govern inevitably means "to conduct someone"[15] to behave in a certain way, the *stimulus-response* mechanism becomes the foremost psychological technique with which to fashion and sustain *homo economicus* as producer and consumer in his need to adept to and adopt today's society of control. But that society in Deleuze's perspective is not only one in which the:

> code is a password... (as much from the point of view of integration as from that of resistance). Where the numerical language of control

[10] Gilles Deleuze, *Negotiations* (New York: Columbia University Press, 1990): 136.
[11] Foucault, *Lectures at the College de France,* 219.
[12] *Ibid.* 218.
[13] *Ibid.* 10-11.
[14] *Ibid.* 270.
[15] *Ibid.* 121.

> is made of codes that mark access to information, or reject it.

It is also the social environment in which "Individuals have become *'dividuals',* and masses, samples, data, markets, or *'banks' "* and where "the man of control is undulatory, in orbit, in a continuous network".[16]

Deleuze's assessment fits "Haley", a social network enthusiast cited in a *New York Times* article[17] who naively expresses one of the chief Orwellian goals of surveillance and control:

> It's like I can distantly read everyone's mind, ...I love that. I feel like I'm getting to something raw about my friends. It's like I've got this heads-up display for them.

Sure, this does not have to be sinister despite Haley's act of surveillance by which he, the surveillant gains power over the surveilled, through the gathering of information regarding that person which they would rather keep secret (or, at least, keep control over its distribution). After all, Haley shares his feelings and opinions on Facebook, shares them with friends "joined to another in mutual benevolence and intimacy", as Ben Johnson once said of friends. Haley might even tweet them to arrange "a social" where they, due to the digital ambient awareness created between them, can skip the introduction and move straight to a discussion of whatever might concern them. The only question is who besides the invisible algorithms of Facebook or Twitter reads Haley's mind when he reads that of his friend? Is his new smart-phone "app" "geo-tagging" him by analyzing his Tweets, Facebook posts, and Flickr stream so as to generate a map of where he and his friends are, as well as the specific locations they frequent? And who tracks, monitors, controls and permanently retains forever their mounting casual bits of information? Not only corporations and marketing conglomerates are heavily invested in it, but individual employers check Facebook to vet job applicants, and some have rejected applicants based on research via search engines and have even been known to fire their employees over posts they have made.

According to Ari Melber's insightful article "The new look of surveillance", younger users of the Internet don't particularly care about who gathers, records, and archives their Tweets and Profiles. More importantly:

> social networking sites are rupturing the traditional conception of privacy and priming a new generation for complacency in a surveillance society.[18]

[16] Deleuze, *October* 59, 3-7 [4].

[17] http.//www.nytimes.com/2008/09/07/magazine/07awarness_t.html-r=1 .

[18] *The Nation:* http://www.alternet.org/story/72556/facebook%3A_the_new_look_of_

Adapting to "soft" surveillance and adopting its parameters of control like Haley does, I contest, rests upon the twofold paradox of today's Internet universe:

1. Hypertechnology creates the conditions of possibility for frequent positional exchanges between surveilled and surveillant: the observed becomes the observer and vice versa. In order to be part of a particular site's culture, social networks induce users to disclose information, and by allowing users into your circle you allow them to track your moves on Facebook together with your interactions with other users, all from your own user page. "You can play with your privacy settings to prevent this, but as you become acculturated to the site, you realize that you have to give information to get information".[19]

2. Social networking sites in particular disseminate information more effectively than other forms of communication including e-mail because it is quicker to simultaneously and instantly message greater numbers of people. And besides conjoining Deleuze's '*dividuals*' in cyberspace the Internet facilitates communal action. Yet the very efficacy with which we connect to the world with hitherto unheard of speed also seduces us to acquiesce and collude with the market place and its aggressive use of private information. No doubt Google and Facebook users can be citizens, share communication and work collectively to build a different world as evidenced by the socio-political upheavals generally referred to as the "Arab Spring" that are interpreted widely as grassroots democratisation. No doubt the Google banner head that states "the web is what you make of it" is true but it leaves unanswered the question: What is the web making of society? By analyzing the Internet and deciphering its messages on the rhetorical plane of what it seduces it users (clients) to do we might be able to better place online activities within a (Foucaultean) general technology of power that in societies of control either moulds citizen-subjects or mutates them into docile consumers.

Given the globally rampant use of such social networking platforms as Facebook, Twitter, and others, the issue becomes increasingly one of "privacy". Whereas current German debates[20] focus on the constitutional

Surveillance .

[19] *The Nation:* http://www.alternet.org/story/72556/facebook%3A_the_new_look_of_Surveillance .

[20] See the influential weekly, *Die Zeit*, http://www.zeit.de/digital/datenschutz/2011-11/verfassungsgericht-facebook and TV news: http://www.tagesschau.de/inland/facebookbundestag100.html .

right of a citizen to be in control of all the data s/he has generated the United States views privacy as a question of consumer protection whereby a disclosure requirement similar to nutrition labels on packaged food "could simply require social networking sites to display their broadcasting reach prominently when new users post information".[21] However, communication protocols of this kind ignore the fact that privacy does not exist in hypertechnological, thoroughly digitised social milieus centred on *homo economicus* and the *subject as consumer*. As Melber states:

> privacy does not matter to children who were raised in a wired celebrity culture that promises a niche audience for everyone. Why hide when you can perform?[22]

Moreover, societies of control effectively blur the domains that for Habermas[23] constitute the "private sphere", the realm of commodity exchange and of social labour, and the "Sphere of Public Authority" that dealt with the State, or realm of the police, and the (bourgeois) ruling class. *Öffentlichkeit* (the public sphere) proper as the discursive space in which individuals and groups congregate via the print media to discuss matters of mutual interest and, where possible, to reach a common judgment through the vehicle of public opinion is inhabited increasingly and almost exclusively by a borderless Internet, a terrain that is limited only by the algorithm. Privacy arguments fail to think the border as decisive part of the conceptual pairing *public – private*, a binary that derives from a spatial distinction between places of general, 'open' social interaction and the *locus* of intimate commerce associated with print culture in the *oikos,* or domestic sphere, shielded from the Panopticon. Not only are my friends and my most intimate thoughts public once committed to the web, it is also no longer the question of what people I know and control but how many people know about it.

In short, "soft" surveillance in societies of control entails numerical, quantifiable access to information by way of prohibition and regulation not qualitative spacing. At stake before a horizon of increasingly controversial data retention regimes are my right to access and control stored data not just in the "memory" of my mobile "machine", the laptop or phone but on the server. Moreover, in an age of receding print culture and new mnemotechnologies in respect of the ways in which I inscribe data and am inscribed by that of others which is then multiplied and transmitted

[21] Ari Melber, *The Nation*: http://www.alternet.org/story/72556/facebook%3A_the_new_look_of_surveillance .

[22] *Ibid.*

[23] Jürgen Habermas, *The structural transformation of the public sphere: An inquiry into a category of bourgeois society*, Thomas Burger and Frederick Lawrence, trans. (Cambridge, MA: MIT Press, 1989).

electronically, there needs to be besides an investigation into discourses on speed and quantity, an analysis of discourses on memory as regards modes of retention and forgetting. Memory, after all is one of the five Aristotelian categories of rhetoric; and what is needed is a politics of memory (and forgetting) that is a politics of the archive: who assembles it for whom and who controls it. Assisted by hypertechnology as condition of "soft" surveillance, rhetoric's persuasive audience appeals tend to avoid *logos* and deliberation, being more often than not reduced to *pathos* so as to produce affect and comply with the apparently benevolent control of our memory by the market. It has to be remembered though, that the seducers are smooth operators not interested in equitable exchange but in "stimulating" a "response" by way of submission.

University of Pretoria