

From Panopticism to Pleasure:

Surveillance, Search and Consumerism in Google's Information Empire

Submitted by Alexander Mahan (33021238) in partial requirement for the degree of MA in Media & Communications in the Programme in Contemporary Cultural Processes, Goldsmiths College, University of London, 2007

Table of Contents:

I. Introduction page 3

II. Overview of Panopticism and Literature Review page 9

III. Google's Mission and Ideology page 15

IV. Outlining Online Surveillance page 23

V. Surveillance Issues in AdWords and Gmail page 32

VI. Surveillance Issues in Google Earth and Google Street View page 38

VII. Privacy, Consumerism and Pleasure page 47

VIII. Resisting the Panoptic Gaze page 52

IX. Conclusion page 57

X. Bibliography page 60

I. Introduction

Everyday living in 21st century consumer society entails frequent encounters with complex and commonplace systems of surveillance. For example, a seemingly innocuous afternoon trip to the supermarket may require the deployment of several surveillant devices: an RFID¹-based transit card (such as Transport for London's Oyster card) for the bus ride down the hill, a credit or debit card for any financial transactions, and often a shopper/consumer card which tracks one's purchases in order to accumulate 'points' which can later be exchanged for various goods or rewards. Many of these activities also take place under the gaze of the ubiquitous CCTV camera, especially in the UK and especially in the nation's capital. A 2002 research project estimated the number of CCTV cameras in London at 500,000 – or approximately one camera for every fourteen people in London (McCahill & Norris 20) – a number which has surely increased in the years since McCahill and Norris conducted their research and since the bus and tube bombings of July 7, 2005. A tourist or resident in Central London can expect their image to be captured hundreds of times in a day (McCahill & Norris 17-19) by CCTV networks on the Tube, on the bus, at stations, in shops and businesses, at tourist destinations, in art galleries, or on the road. On the surface, these systems may appear as disparate technological entities; arrangements that are occasionally irksome but necessary and perhaps even pleasurable components of modern urban living. We enjoy the convenience of cash-free transactions, the speediness of key-free entry into cars and apartments and the paper-free exchanges of online banking and automatic billing services. However, as David Lyons notes in 'The Electronic Eye - The Rise of Surveillance Society', these systems are not simply tools for single

¹ Radio Frequency Identification Device

transactions – they also store details about each operation in large databases of information which can then be indexed, searched, cross-referenced, distributed, and even perhaps sold by those who administer the database:

“In each case mentioned, computers record our transactions, check against other known details, ensure that we and not others are billed or paid, store bits of our biographies, or assess our financial, legal or national standing. Each time we do one of these things we actually or potentially leave a trace of our doings. Computers and their associated communications systems now mediate all these kinds of relationships; to participate in modern society is to be under electronic surveillance” (Lyons 4).

In addition to these ‘everyday’ technologies of information surveillance, our ‘online’ activities and exchanges – reading and writing e-mail, browsing the web, searching, instant messaging, posting in forums, publishing blog posts, leaving comments, uploading photographs – are also subject to various forms of surveillance, or ‘dataveillance’², enabled by powerful database servers with ever-increasing processor speeds and large storage capacities, and networks that allow for the almost instantaneous flow of data around the globe without regard for national boundaries. In the networked information society, capacities for individual and collective dataveillance increase daily. In advanced capitalist societies in particular, surveillance is frequently used by business and corporate interests in order to gather information on consumers for marketing and commercial purposes.

² ‘Dataveillance’ is the term used by Australian computer scientist Roger Clarke to describe the rapid increase in the quantity of surveillance in computerised societies, brought about by technological convergence in computing and the inherent (re)configurability of digital communications systems (Lyons 48).

This seemingly constant state of personal and informational surveillance in contemporary society raises a number of important questions: who is in control of surveillance technologies, and who has access to the information gathered by these technologies? What are the ethical issues surrounding surveillance? How is power and social control manifested in surveillance? There have been many studies of surveillance that attempt to answer these questions³. Most of these enquiries have typically centred on ‘hard’ technologies of surveillance such as CCTV, wiretapping, ID cards, state-implemented welfare and taxation systems, banking and credit databases, etc. These forms generally exist as regulatory, disciplinary or deterrent measures implemented by governments and corporations in order to discourage and prevent undesirable or illegal activities (CCTV, wiretapping), to monitor financial transactions and records (banking and credit databases), to keep tabs on individuals and populations (passports, ID cards, work and residency visas), and to gain and share personal information such as addresses and telephone numbers for purposes of direct marketing (‘junk’ mail, catalogues, marketing calls, etc). Understanding these commonplace forms of surveillance is of critical importance to questions of social control. However, the rise of the Internet and the World Wide web in the last decade as a medium of mass communication presents new and relatively unexplored territories for studies of surveillance, and it is within this surveillant landscape that I present this enquiry. In this paper, I will argue that surveillance in the informationalised postmodern consumer society is becoming increasingly ‘softer’ – less a technology of top-down centralised regulation and discipline than, to summarise Michael Hardt and Antonio Negri in ‘Empire’, a function of deterri-

³ See Lyons, McCahill, Foucault, Mann, Manovich.

torialised capital which produces subjectivities within the global network of communicative capitalism (23) – subjectivities which can be ‘democratised’ and ‘pleasurable’ rather than disciplinary. While surveillance certainly remains a mechanism of social control in postindustrial society, the networked society of control as opposed to the disciplinary society is a distributed, ambiguous control rather than an institutionalised site of bodily discipline:

“The society of control might thus be characterized by an intensification and generalization of the normalizing apparatuses of disciplinarity that internally animate our common and daily practices, but in contrast to discipline, this control extends well outside the structured sites of social institutions through flexible and fluctuating networks” (23).

How is the society of control manifested in online activities and identities? More generally, does the informationalisation of society and the availability of ubiquitous communication networks *increase* the disciplinary function of surveillance or make it more ‘transparent’ and ‘democratic’? Is contemporary society doomed to an inescapable surveillant dystopia (a la *1984* or *Brave New World*) brought about by the totalising effects of inherently capitalistic communication systems, or are there possibilities of resistance and autonomous spaces in the realm of networked communication technologies? In this paper, I will discuss these questions with particular reference to Google’s Internet search engine and also Google’s suite of software applications, specifically Gmail, Google Earth and Google Street View. I’ve chosen Google as a case study for this essay because of the company’s well-documented market domination in web search and Internet advertising, its dependence upon dataveillance and surveillance to provide many of its services, its

global reach, and its seemingly ‘benevolent’ and ‘democratic’ (the informal motto of Google is “don’t be evil”⁴) corporate mission to “to organize the world’s information and make it universally accessible and useful”⁵. By researching the use of surveillance in Google’s web searching tools and in its online applications, I hope to develop a critical perspective that is neither blindly utopian nor darkly dystopian in its approach to surveillance.

To begin this line of questioning, I will briefly outline the theory of Panopticism, Michel Foucault’s critical application of Jeremy Bentham’s prison design as both physical structures of societal control and also as metaphor for power relations and social control. Following this discussion of Panopticism, ‘Discipline and Punish’ and other relevant literature used in the essay, I will present a short outline of Google’s corporate mission and operational ideology and then a summary of common forms of online/Internet surveillance in order to provide a practical background from which to explain how Google uses surveillance in its various virtual products. The remainder of the essay will be devoted to critically investigating the uses of surveillance in Google search, Gmail and Google Earth and addressing ethical and social questions which arise from the operation of such processes.

⁴ <http://investor.google.com/conduct.html>, accessed 14 Aug 2007

⁵ <http://www.google.co.uk/intl/en/corporate/index.html>, accessed 14 Aug 2007

II. Overview of Panopticism and Literary Review

Many studies of surveillance understandably begin with a Foucauldian reading of the ways in which surveillance plays a significant role in enabling social control and how power is inscribed into both the individual and the social body. In ‘Discipline and Punish’, Foucault describes the historical shift from highly visible, public methods of corporeal punishment – such as public executions and torture, the stocks, chain gangs, etc – to a society in which punishment becomes “the most hidden part of the legal process” (9). Punishment as spectacle receded from view over time and in its place appeared frameworks of penal and judiciary codes, moral assessments and judgements, and state-constituted principles of ‘normativity’ which sought to establish certain discourses of acceptable and unacceptable behaviour. Power and social control became less dependant upon being exercised directly on the body through pain and torture and more reliant upon discipline through subjection to mechanisms of observation, training and correction. As Foucault notes, “In physical torture, the example was based on terror: physical fear, collective horror...The example is now based on the lesson, the discourse, the decipherable sign, the representation of public morality” (110).

Foucault uses Jeremy Bentham’s ‘Panopticon’ prison design to illustrate how these new systems of discipline were (and are) instituted and distributed throughout society. Bentham’s original design for a Panoptic (meaning ‘fully visible’ in the original Greek⁶) prison is one in which cells are arranged in a circular pattern around a central watch tower. The guards in the tower can easily monitor the residents of the cells, but the prisoners can neither see each other nor the guards in the watch tower, thus ensuring a constant state of being seen but not seeing: “in the pe-

⁶ Source: <http://www.thefreedictionary.com/panoptic>

ripheric ring, one is totally seen, without ever seeing; in the central tower, one sees everything without ever being seen” (202). Such an arrangement creates a permanent state of visibility and a self-conscious subjection to power, as the prisoners are aware that they may be under the gaze of the guard at any time, thus inscribing in themselves the responsibility of behaving accordingly to the constraints of rules (202). In the Panopticon, the idea of being watched is internalised, subjects become self-regulating, and power functions automatically.

Foucault extends the application of this surveillance-based system of control to various social institutions: the hospital, the school, the factory, the barracks. In each case, observational mechanisms serve to order bodies in space and structure relations according to disciplinary discourses. The Panopticon doesn't exist solely to reform prisoners, but “to treat patients, to instruct schoolchildren, to confine the insane, to supervise workers, to put beggars and idlers to work” (205). Additionally, the Panopticon is not simply a building or a design for a physical location; it is a distributed mechanism of power: “its functioning, abstracted from any obstacle, resistance or friction, must be represented as a pure architectural and optical system: it is in fact a figure of political technology that may and must be detached from any specific use” (205). Rather than a punitive structure such as the torture-filled spectacles or the public shamings of the past, panoptic power is a method of social regulation and organisation; of subjectivities produced through disciplinary discourses.

Panoptic theory thus lends itself aptly to current studies of surveillance and social control. In the web of everyday surveillance in which we presently find ourselves, we can certainly find powerful connections between modern technologies of

surveillance and social ordering, in the ways in which discourses of inclusion and exclusion are shaped and organised under the gaze – under the gaze of hundreds of thousands of CCTV cameras in London; of Social Insurance and Social Security Numbers (and their corresponding rights and privileges); of credit reports and financial histories; of workplace surveillance of employee web and e-mail usage, etc. However, despite the usefulness of Panopticism as a concept in exploring issues of power and social relations in surveillance, we must be careful to avoid an all-totalising account of ‘Surveillance as Panopticon’, as not all surveillance is necessarily panoptic, not all power is in the hands of centralised institutions, and sometimes, as we will discover later, the ‘gaze’ can be resisted and even turned back on those who seek to wield power over ‘subjects’. As Mark Winokur notes in ‘The Ambiguous Panopticon: Foucault and the Codes of Cyberspace’:

“Neo-Foucauldian cultural critics understand surveillance society as a top-down phenomenon in which an otherwise scarcely visible oligarchy utilizes new technology as a tool of social surveillance. They understand panoptic society to be a sort of Orwellian 1984 or Kafkaesque Castle in which power is invested in the powerful if invisible.”

While it is important to find a position of informed scepticism with regard to the rise of surveillance technologies in everyday life, perhaps we don’t need to locate ourselves in a ‘Foucauldian dystopia’ in which all social activity is carefully monitored and controlled by a centralised Big Brother. Indeed, in modern communications networks, the disciplinary mechanisms of the Panopticon are giving way to more subtle and decentralised systems of control. Thus, I turn to ‘Empire’ by Michael Hardt and Antonio Negri to explain some of the more recent manifestations

in the society of control. In 'Empire', Hardt and Negri describe the shift from imperialism to Empire, the move from disciplinary society to biopolitical production in the society of control. For Hardt and Negri, communication networks and globalised capitalism go hand in hand. Instead of institutionalised sites of discipline – the hospital, the prison, the school – we have global, deterritorialised information in the service of postmodern capitalism. and networks as 'rhizomatically inter-linked fibers of being' (Dean 265).

In addition to 'Empire', I refer often to David Lyon's book 'The Electronic Eye: The Rise of Surveillance Society'. This work provides a comprehensive and balanced sociological background of surveillance which informs much of the backdrop to this research. Rather than taking a binary 'good versus bad', 'optimistic versus pessimistic' approach to surveillance and society, Lyon's study is presented from a point of view which is understandably sceptical of the rise in surveillance technologies but also willing to reach beyond paranoia or fatalism to provide an ethical and practical response to pervasive contemporary surveillance.

Throughout this essay, I also refer to 'The Search' by John Battelle to provide important practical and historical information about Google's revenue models, corporate ideologies and business practices. While 'The Search' is primarily a book about business rather than a theoretical or sociological text, I believe that it's helpful to seek an understanding of the operational characteristics of businesses before attempting a critique of their practices.

To provide many of the statistics and recent commentaries on Google and information surveillance in this paper, I use various web sources such as Internet

research firms, technology and privacy blogs, personal blogs, online newspapers and magazines, and critical online-only journals such as ctheory.net. In an informational realm where technologies shift in the blink of an eye and many insightful essays are content to live in digital form rather than print, web sources are vital to receiving up-to-date and relevant observations on web culture.

Additional useful texts cited in this paper include 'Ctrl Space: Rhetorics of Surveillance from Bentham to Big Brother', a collection of essays and art projects which critically engage with various surveillant discourses, 'Freedom' by Zygmunt Bauman and 'Empire's New Clothes', a collection of commentaries on Hardt and Negri's 'Empire.'

Building on these key texts and resources, we can now begin to examine more closely the specific techniques of information surveillance employed by Google and their implications for ethics, privacy, consumerism and social control.

III. Google's Mission and Ideology

As noted earlier in this paper, Google's corporate mission statement is "to organize the world's information and make it universally accessible and useful." Google uses its massive investments in research, human capital, and server and network infrastructure to build frameworks by which information of all types can be created and collected, indexed, ordered, stored, parsed, located and retrieved. While perhaps best known for its Internet search engine⁷, which currently dominates the worldwide market for web search⁸, Google also provides a large number of other online services and applications that relate to the mission of 'organising the world's information'. Google Maps and Google Earth allow for all kinds of information to be combined, graphically represented and searched in a geospatial context. Google News links to hundreds of news sources around the globe via a complex algorithm that chooses the most 'popular' and 'relevant' news stories at the time of the search. Google Scholar searches through myriad journals and research communities to find academic papers, articles, and abstracts. Blogger.com (a blogging company owned by Google) hosts hundreds of thousands of blogs, YouTube (a recent Google acquisition) hosts and serves streaming online video and Gmail, Google's web-based email service, provides email to approximately 60 million users around the world (Blanco).

All of these services and the possibility of achieving 'the organisation of the world's information' are reliant upon the ability of Google's servers to systematically collect, classify and distribute data from an immense number of points across

⁷ The popularity and success of Google's search engine created a new verb: 'to Google' for something is 'to search online' for something.

⁸ Google searches currently account for around 55% - 65% of all U.S. web searches ('Search Engine Market Score' and 'Leading Search Engines') and approximately 70% of the global search market (Jarboe).

the global network of the Internet. This automated, algorithmic process of attempting to monitor and map the flow of the world's information is a massive project of dataveillance. While dataveillance is not necessarily inherently panoptic – data can be collected for reasons other than social and individual control and arguably, data in itself is not a 'disciplinary discourse' that exists to 'constitute subjects' – enquiring into the forms of Google's surveillance and the ethical/social issues that are related to such surveillance is vitally important, especially given that Google is the largest and most financially successful search company to date. When so much information (both 'private' and 'public' information) is in the hands of one corporation, and the corporation's business model involves attaching commercial advertising to that information, the potential for power (both 'hard' and 'soft') looms large.

The Mind of God

Google has a grand, universal vision for its business of organising information. In an informal 2002 dinner interview with the business magazine *Red Herring*, Google co-founder Sergey Brin was quoted in response to the question "what would the perfect search engine look like?" as saying "It would be the mind of God...Larry [Larry Page, Brin's founding partner] says it would know exactly what you want and give you back exactly what you need" (Willison, 2002). Another oft-repeated Google catch phrase is 'Don't Be Evil,' the unofficial corporate motto which came about during a 2001 brainstorming session to determine the fledgling company's core values (Battelle 138).

By using the moralistic language of 'Good' against 'Evil' and by comparing their ideal search engine to 'the mind of God,' Google presents itself as some sort

of divine and benevolent technological entity – while it may admit to be all-seeing and all-knowing, the language suggests that Google has the best interests of the consumer and indeed the best interests of the whole world at heart: who *doesn't* benefit from quick and comprehensive access to the world's information databases? However, this sort of language is profoundly problematic, and not just because of the difficult task of defining which actions are 'good' and which are 'evil' for a company whose business is the structuring of the world's information and attaching advertising based on keyword relevance⁹. The totalised notion of a 'divine' computerised gaze presents additional concerns of surveillance and social control. By comparing their ideal search engine to the mind of God, Brin and Page reveal a desire to (re)create perhaps the world's earliest and most ubiquitous mechanism of control: the totalitarian Eye of God. In 'The All-Seer: God's Eye as Proto Surveillance', Astrit Schmidt-Burkhardt describes the hegemonic function of the ever-present 'Eye of God' throughout religious and social history. The symbolic idea of the divine gaze has often been employed to set moral and ethical boundaries, encourage 'normal' behaviours, establish methods of salvation and punish 'wrongdoers' (18-23). More recently, however, the singular gaze of God has given way to the networked technological gaze of computers and other surveillant devices: "In this systemic shift from hegemonial gaze to Deus ex machina, God is being replaced as the paradigmatic world observer by increasingly perfected techniques of illustrating the visible and invisible reality" (31).

⁹ For instance, in January, 2006, Google decided to open a portal in China which filters search results according to Chinese government policies. The company understandably received large amounts of flak online and in the popular media for the decision, which appeared to compromise their ethical commitment to 'not being evil'.

The language of answering ‘wants’ and providing ‘needs’ reflects this shift – instead of receiving spiritual provisions from the divine hand of God, we request and receive valuable information from Google. But for Google to understand our requests and dispense information accurately, we must submit to patterns of surveillance in order for the technology to ‘get to know us better’. For most of us, those who best know our wants and needs in life are those with whom we share some sort of emotional or intimate connection: friends, family, romantic partners, etc. We are willing to divulge personal information and engage in conversation with others because there’s a reciprocity of trust that the other party won’t share your thoughts and words with others without permission. For Google to know your wants and needs, or perhaps more accurately, in order for Google’s mathematical algorithms to ‘predict’ your wants and needs in searching, its database must be able to construct a detailed profile of your online behaviour, search history, products purchased and geographic location, and connect all of this information to a specific identity.

This is known as the ‘clickstream’, the virtual trails and tracks that one creates while clicking from site to site, a journey through the web which forms a kind of narrative thread about the user’s intents and desires as they search for information, entertainment, images, news, pornography, etc (Battelle 257). The more information about the patterns of this ‘clickstream’ that can be gathered and analysed, so the logic goes, the more personally relevant search results and any accompanying advertising can be in the future. For example, Google’s recently released ‘Web History’ tool allows for users with a Google account and the Google Toolbar installed in their web browser to sign up for a service that indexes all web

activity for future searchability and archival purposes. As a Product Manager writes on the official Google blog, “Web History lets you look back in time, revisit the sites you've browsed, and search over the full text of pages you've seen. It's your slice of the web, at your fingertips” (Shodjai, 2007).

But Web History is not simply ‘your slice of the web.’ It’s also Google’s index of your online behaviour. By observing these detailed records of web user behaviour, Google and other search companies will be able to deliver increasingly personalised content and promise advertisers the ability to serve ads to exponentially smaller target markets – in theory, businesses could specify ‘a 34-year-old single female who works in investment banking, lives in Manhattan, and who has been searching for new kitchen appliances in the last week’ and choose to purchase pay-per-click advertisements from Google to be served only to that particular demographic. To be able to monetise the clickstream and target advertising individually is the Holy Grail of Internet commerce. In the domain of commerce, Google’s economic goals are equally as totalised as its informational goals – the two are certainly complementary in the networks of the information society. Just as Google wishes to order and provide access to all of the world’s information, it also desires to include the entire world economy in their informational empire. In John Battelle’s book ‘The Search’, he outlines the history of online search and the ways in which Google aims to utilise supply and demand in the information economy to continue the rapid growth of their business. Google’s understanding of the market for information is that demand is ‘one bit of computable information’ and supply is another. Thus, for those who are able to match the two together, there exists a

potential market for the entirety of the world's information (248). As Battelle explains:

“If you add in every small business in the world—and believe me, Google is thinking that way—you can sum up Google's ambitions in the commercial world as this: the company would like to provide a platform that mediates supply and demand for pretty much the entire world economy. As [Google CEO Eric] Schmidt put it, ‘The sum of [Google's addressable] market, if you include in the large companies and the small companies throughout the world, is the world's gross domestic product’” (248).

It appears that Google is making strong progress on its way to achieving this goal. In 2006, Google received net income of \$3.6 billion on \$10 billion in revenue, an amount larger than the GDP of many developing countries (‘IMF Report’, 2007). 99% of Google's income in that same year came from advertising revenue (‘Fiscal Year 2006 Results’, 2007) – mostly from the small, text-based advertisements such as the column of ‘Sponsored Links’ that appear above and to the right of many search results. While most of Google's advertising has traditionally taken the form of these text-based keyword ads, the company's recent acquisition of the Double-Click ad serving network gives it the additional capability to work with graphical, image-based and animated advertising. Text-based ads currently make up about 40% of web advertising, and display or graphical ads make up another 40% (‘IAB Internet Advertising Revenue Report’ 9), so the display ad market is a lucrative entry for Google.

Google understands both its advertising programmes and its model for web search as ‘beneficial for the consumer’¹⁰ and representative of the ‘democratic nature of the web.’¹¹ However, as I will outline in the next chapter, much of the web lends itself toward new techniques of surveillance, and it’s important to keep this in mind when confronted with this type of techno-utopian rhetoric, especially from a company with the informational power of Google.

¹⁰ “In short, Google’s acquisition of DoubleClick will benefit all parties in the online advertising business, including advertisers, publishers, agencies and, most importantly, consumers.” (Kinnier, 2007)

¹¹ Source: <http://www.google.com/technology/index.html>

IV. Outlining Online Surveillance

The vast amount of information available on the Internet and the ‘hidden’ or ‘invisible’ methods available to sort and track information and individuals lends itself to various forms of online surveillance. What follows are several descriptions of the practical ways in which surveillant techniques are implemented and used online, all of which are used by Google or by users of Google’s services in one way or another.

The use of ‘cookies’ by websites

Many websites leave ‘cookies’ on the hard drives of web users – small pieces of textual data which are sent from the server to the browser in order to be employed for purposes of user identification, authentication, personalisation, and online commerce. For example, if one creates an account with an online shopping site, adds a few products to a shopping cart, and subsequently browses away from the page or closes the browser window, the shopping site can use a cookie to ‘remember’ the login details and contents of the shopping cart unique to that user. Cookies can also be used by sites to track which pages are visited within the site in any given session or by third party advertisers to create an anonymous user profile in order to serve varying banner advertisements based on that profile¹². According to its privacy policy¹³, Google uses cookies to store user preferences and track user trends in order to find out how people search. Most web browsers allow users to turn off or delete cookies as a preference setting, but many web surfers are either unaware of their presence completely or don’t really understand their function. According to a 2005 study, around 25% of surfers ‘don’t know’ what cookies are and

¹² Source: http://en.wikipedia.org/wiki/HTTP_cookie#Tracking (accessed 7 August, 2007).

¹³ Source: <http://www.google.co.uk/intl/en/privacypolicy.html#information> (accessed 26 August 2007).

of those surfers who are aware of cookies, around 50% are unsure of how they function (Quinton).

Workplace Internet surveillance

A growing number of employers use various combinations of hardware and software to monitor and control web and e-mail usage in the workplace. Visiting 'inappropriate' websites or recreational web browsing, writing personal e-mails on company time, criticising co-workers or company policies, releasing sensitive corporate information, or downloading illegal software, among other behaviours, may all lead to disciplinary measures. For example, in February, 2002, popular blogger Heather Armstrong was fired from her web design job after administrators read negative comments about the company on her website (Armstrong), thus leading fellow bloggers to coin the term 'Dooiced' – to be firing for talking about work in a personal blog (Waters). A 2007 survey of 308 companies with over 1000 workers found that 32% of the companies employ staff to monitor outgoing employee e-mail, 46% have disciplined employees for violating e-mail policy, and 19% have disciplined employees for violating blog or message board posting policies (Coombes, 2007). Another 'disciplinary' mechanism is the use of web search to pre-screen potential employees as many employers and recruiters are using Google to screen and eliminate job candidates by searching for relevant online information linked to the candidate's name ('Digital Dirt', 2007).

Search as surveillance

Typing the name of a new acquaintance, potential employee, old friend, or romantic interest into a web search engine to discover details about their personal histories and current interests is a relatively recent phenomenon in surveillance. The

power of search engines to rapidly aggregate data and connect various types of digital information in an easy-to-use interface presents us with unprecedented possibilities for individual and social surveillance, possibilities that certainly appear Panoptic in their ability to institute and govern social relations – without the knowledge of the person under surveillance, we may ‘subject’ them to a keyword-based enquiry that opens up personal information and a history of working relations in order of relevance (Albrechtslund, 2006). In addition to textual and keyword-based searches for individuals, products such as Google Earth and Google Street View allow for searching, ‘zooming in’, bookmarking, and annotating physical locations on the surface of the Earth.

Commercial surveillance for marketing and economic purposes

Businesses with an online presence have a massive commercial interest in creating detailed profiles of individuals and user groups in order to more accurately target marketing and advertising, sell products, create content, and direct traffic to maximise revenue. With the successful rise of popular ‘social networking’ sites such as Myspace, Facebook, Flickr, and Last.fm, businesses have a rich collection of personal data from which to draw upon, especially from the desirable social groups of teenagers and young adults, who tend to be on the cutting edge of cultural trends and who have a relatively large amount of disposable income. User profiles on these various social networking sites often include such information as age, location, gender, personal interests and hobbies, educational level, field of employment, sexual preference, and religious and political views. While it is up to each user to decide which details to make public and which to keep private, and although most social networks have privacy policies in place to prevent the sharing

or sale of personal information to third parties, this type of information can be collected into databases, sorted, and used to tailor specific marketing messages to specific profile matches. Rupert Murdoch's News Corp.'s \$580 million acquisition of Myspace.com in July, 2005 (Siklos, 2005) is widely viewed as a shrewd business manoeuvre because of the valuable user information obtained in the transaction. Online shopping sites such as Amazon.com track previous purchases and page viewing history in order to provide 'personalised recommendations' to users – for example, if I purchase a book about how to code a website with XHTML, Amazon may recommend similarly branded web design and development books upon my next visit to the site. As I buy additional products and services, Amazon uses this information to construct and continually update a consumer profile based on my purchasing habits. This profile of personal information (location, age, gender, income level) combined with a history of the user's consumption patterns and spending habits enables Amazon and their partners to generate extremely specific marketing messages and offers¹⁴. Google uses a similar process of profiling and customisation in targeting their commercial advertising and marketing messages, as I will shortly describe in an analysis of Google's AdWords programme and Gmail. Perhaps more nefariously, commercial spammers use software and hardware 'robots' to scour the underlying HTML code of websites in order to harvest unencrypted e-mail addresses for their spam mailing lists.

¹⁴ "Amazon.com also displays targeted advertising based on personal information about users. Although Amazon.com does not provide any personal information to advertisers, advertisers (including ad-serving companies) may assume that users who interact with or click on a targeted advertisement meet the targeting criteria used to display the ad (for example, users in the north-western United States who like classical music)." <https://www.amazon.com/gp/help/customer/display.html/105-0913240-4018048?ie=UTF8&nodeId=468496&type=&token=&jsEnabled=&as=4>

Self-surveillance

Related to the popularity of ‘social networking’ online is the trend toward ‘self-surveillance’ or ‘self-disclosure’; that is, making large amounts of previously private or personal information freely available in the public realm. In the user profiles of social networking sites such as MySpace and Facebook and in myriad personal blogs, we see a great number of people choosing to reveal discourses and narratives which were formerly mostly private – diary entries, photo albums, videos of self, friends, and family, sexual desires and preferences, geographic location – all of these are now indexed, searchable, and easily obtainable. While the majority of such websites do offer privacy controls which allow the user to select which information is ‘public’ and which remains ‘private’¹⁵, and have substantial privacy policies (privacy policies generally outline what types of information the site collects about users, what that information is used for and with whom it is shared), it appears that many users are willing to forgo traditional notions of privacy for the social benefits that such transparency affords: making new friends, archiving personal experiences and sharing those experiences with others, creating business opportunities, promoting music and art, etc. In Emily Nussbaum’s article ‘Say Everything’ for New York magazine, she investigates this relatively recent phenomenon of online self-disclosure and found that young people’s attitude toward ‘privacy’ differs vastly from that of previous generations. According to Nussbaum, while middle-aged parents and media commentators fret about ‘stranger danger’ and online stalking, teenagers and people in their 20s are embracing the social benefits

¹⁵ For example, Myspace and Facebook both offer the ability to hide one’s profile from strangers (people that haven’t been approved as ‘friends’), and it’s up to the individual user to decide which pieces of information are made available for public consumption.

and pleasures of online networking and archiving. Since we are all under constant surveillance in consumer society already, so the argument goes, why not ‘make ourselves public’? Nussbaum links this new ‘publicness’ of personal information to various life opportunities: “All sorts of opportunities – romantic, professional, creative – seem to Xiyin to be directly linked to her willingness to reveal herself a little” (29). Many people growing up today continually document their thoughts and every day lives online and are quite comfortable with the ubiquitous digital presence of personal information and images – only a Google search away from future employers or romantic interests. Of course, the type of personal information made public on social networking sites also presents a commercial cornucopia for marketers and media firms, as is evidenced by the aforementioned purchase of Myspace by Rupert Murdoch’s News Corp, the \$260 million purchase of Last.fm by CBS (Allen, 2007), the acquisition of YouTube by Google and the acquisition in 2005 of photo sharing website Flickr.com by Yahoo (Hu, 2005).

Governmental surveillance

Governments worldwide have many surveillant mechanisms in place to monitor web traffic for illegal activity, security breaches, terrorist ‘chatter’, and ‘subversive’ content in general. There are a variety of techniques that can be employed, from the ‘Great Firewall of China’ in which the Chinese government monitors web traffic and blocks access to many sites and networks considered ‘undesirable’ or ‘dangerous’ by authorities (Battelle 204) to the FBI’s much disputed ‘Carnivore’ system, in which web traffic and e-mail can be intercepted, logged and monitored for ‘intelligence’ purposes. Intelligence officers and private intelligence firms are also employed to observe online forums, discussion groups, and jihadist blogs for conver-

sations related to terrorism, activism, and politics around the world (Thompson, 2006, see also the SITE Institute¹⁶). Drawing on recent ‘collaborative’ projects online, the CIA recently created a collaborative intelligence environment called “Intel-lipedia”, which functions somewhat like the collaborative encyclopaedia Wikipedia but with access limited to intelligence employees with classified clearance (Thompson, 2006).

Many local and national governments also maintain websites listing the identities and whereabouts of known sex offenders and other criminals, allowing law enforcement officials and communities to ‘keep tabs on’ individuals who have committed crimes of a violent and/or sexual nature. In the United States, federal legislation¹⁷ requires each state to release information on sex offenders, and the web is often the quickest way to distribute such information to the public. Oregon’s database, for example, allows visitors to the website to search by street address or postal code, and using the visualisation provided by Google Maps, graphically overlays an icon showing the location of any nearby sex offenders. Once an icon is clicked, a window pops up with information about the offender: recent photo, address, age and physical description, prior convictions, victim types, conditions and restrictions, and vehicle information. Although one can understand the motivations behind such sites – attempting to protect children and women from harm by exposing those in their neighbourhoods and communities who have committed sexual crimes in the past – this type of surveillance is certainly the ‘hardest’ type of exclusionary discourse to be found online. Indeed, governmental

¹⁶ URL: <http://www.siteinstitute.org/mission.html>

¹⁷ This legislation is known as ‘Megan’s Law’, signed into legislation in May, 1996 (<http://www.megans-law.net/>)

online surveillance reveals itself to be the most ‘panoptic’ in the carceral sense of the word.

All of these surveillant gazes can be read in the context of panoptic power: ‘invisible but ever-present’ workplace surveillance to constitute appropriate employee behaviour, commercial surveillance to encourage certain consumer behaviour and purchases, self-surveillance and disclosure to place oneself within certain social groups and networks, government surveillance to monitor and exclude ‘criminals’, ‘terrorists’, or ‘subversives’. Keeping these various manifestations of the gaze in mind, I now turn to several of Google’s online services in order to examine their surveillant qualities and potential for social control.

V. Surveillance Issues in AdWords and Gmail

“It is clear that a search engine which was taking money for showing cellular phone ads would have difficulty justifying the page that our system returned to its paying advertisers. For this type of reason and historical experience with other media, we expect that advertising funded search engines will be inherently biased towards the advertisers and away from the needs of the consumers” (Battelle 92).

As noted earlier in this paper, Google creates revenue by attaching advertising to bits of information. In the initial academic paper introducing Google, however, Brin and Page shied away from advertising out of a concern for its potential to commercially bias search results, as the above quote indicates. But as the fledgling search engine became increasingly popular and the project evolved from an academic project¹⁸ to a commercial endeavour, pressure mounted on the founders to provide a revenue model for the business. In response to this pressure, the company developed a method to separate and delineate paid ads from the ‘organic’ search results, and AdWords was born.

Google’s AdWords programme allows advertisers to create ads and choose keywords and phrases related to the product or service advertised. The advertisers agree to pay a certain amount each time an advertisement is clicked. These advertisements then appear as ‘Sponsored Links’ on the results page when users search for related keywords or in columns of ads on websites that participate in the AdSense programme. Websites using AdSense receive ads from the AdWords network and then share in the revenue stream whenever those ads are clicked. For instance,

¹⁸ Google began in 1996 at Stanford University as Larry Page and Sergie Brin’s computing science project (Battelle 73-80).

a post about wind farms might generate text ads for residential wind turbines or green energy services – the text of the article is automatically parsed by Google’s servers and ads served accordingly. This form of dataveillance is relatively uncontroversial in a market economy, as most forms of media attempt to provide advertising relevant to content, whether one is watching ‘Big Brother’ or reading ‘The New York Times Magazine’. The arrival of Gmail and its accompanying AdWords integration, however, provoked controversy over ‘privacy’ issues and also ushered in a new era in personally targeted advertising served by dataveillance techniques.

Gmail and the algorithmic surveillance of personal e-mail

Gmail is a free web-based e-mail service launched by Google in mid-2004. At that time, most web-based e-mail services (such as Microsoft’s Hotmail and Yahoo e-mail) only offered 10 or 20 megabytes of storage space, while the Gmail service offered 1 gigabyte of storage¹⁹ and an unparalleled search capability, allowing users to archive and search through thousands of e-mails extremely quickly. Gmail uses Google’s AdWords technology to place a column of ‘relevant’ textual advertisements next to the body of the e-mail. For example, an e-mail with content referencing ‘architecture school’ and ‘architecture’ may display text ads related to architectural academic programmes, openings for architectural job positions, or for architecture firms who would like the user to consider their design/build services. Additionally, because the user’s IP address contains information related to geographic location (my current IP address of 158.223.167.217 indicates that I am surfing the web in London, UK²⁰), Gmail is also able to serve location-based adver-

¹⁹ 1 gigabyte is equal to 1000 megabytes; Gmail’s storage allotment increases on an exponential basis and is currently approaching 3 gigabytes or 3000 megabytes. Source: <http://www.gmail.com>

²⁰ Source: <http://www.whatismyipaddress.com/>

tisements. This strategy of targeted, ‘contextually relevant’ advertising placed in personal e-mail initially proved quite controversial, as privacy advocates and commentators saw Google’s technique of monetisation as an unprecedented intrusion into the previously ‘private’ domain of interpersonal communication – the company was accused of ‘snooping’, ‘oogling private e-mails’, abusing consumer privacy, et al (Battelle 195).

Indeed, Gmail marked a new trajectory in market-based observation of personal information. Traditionally, personal letters between individuals have been considered part of the private realm of communication – aside from the unscrupulous mail snoop or an intrusive postmaster, one could be relatively confident that one’s missives would reach their intended recipient unread and free from third party intervention. In Gmail, the line between ‘public’ and ‘private’ is more ambiguous – while employees at Google aren’t ‘reading’ personal e-mail, Google’s computers and algorithms are busy parsing the text of e-mails for relevant matches from the massive AdWords network (Battelle 195), so whether the message is about weddings or funerals, Gmail users will see computer-served textual ads next to the body of their email. Private thoughts and conversations in Gmail are subject to technological surveillance that transforms intimate words into an information commodity – keywords as little commodities, purchased by small and big businesses alike for pennies per click.

However, given the millions of people willing to sign up for a Gmail account, it appears that many users are comfortable with the idea of ‘sharing’ their personal e-mail with Google in exchange for a free e-mail account with large amounts of storage and an innovative search function. Perhaps Gmail users are

willing to let computers parse their personal e-mails and insert advertising because computerised algorithms are anonymous and propagated by ‘non-feeling machines’. In contrast to this, if there were teams of Google employees physically reading e-mails and manually inserting advertisements relevant to the content, people would feel extremely wary about signing up for the service. Here we can see a willingness to submit ourselves and our information to a commercialised technological gaze but not the gaze of human readers. In this sense, we trust computers more than we trust humans; we feel secure under the surveillant gaze of anonymising algorithms.

The aim of AdWords – in search results, on websites and in Gmail – is to persuade users to click on relevant ads and purchase the various products and services advertised. It is a discourse of consumerism that makes up a core part of Google’s informationalised economy. In AdWords, then, we can certainly see panoptic elements – the unseen but ever-present surveyor (Google’s AdWords algorithm which scans the e-mail for keywords), the discourse of control (commercial messages attached to personal information), the self-constituted subject (the user of Gmail, submitting to the commercialisation of personal messages). But rather than being representative of a physical Panopticon as institutionalised site of discipline, Gmail presents a virtualised site of control and economic production, and rather than having the regulatory and punitive characteristics of a prison or a school, Gmail presents a system which can be a useful and pleasurable part of our daily communication habits and patterns. Reading this shift in Hardt and Negri’s terms, this move from discipline to control would be representative of the newly biopolitical nature of power – “Biopower is a form of power that regulates social life from

its interior, following it, interpreting it, absorbing it, and rearticulating it” (23-24). Hardt and Negri see the communication industries and their immaterial production of language and communication as the site of “biopolitical production of order” (32). Social space is synthesised in the space of communication, which produces commodities and subjectivities, and legitimates the dominant modes of production by “developing its own languages of self-validation” (33). Google is not only producing information commodities through AdWords and Gmail, it is also producing producers: “life is made to work for production and production is made to work for life” (32). Next, I will examine how these processes of production and commoditisation are extended in the geospatial representations of Google Earth and Google Street View.

VI. Surveillance Issues in Google Earth and Google Street View

Gmail is a pertinent example of dataveillance for commercial and productive purposes. But Google's surveillant capabilities and services go far beyond the keyword-based dataveillance of Google web search and Gmail. In order to further its mission of universal information organisation and provision, Google (as has its main competitors, Yahoo and Microsoft's MSN network) has expanded the function of its search to include comprehensive digital collections of geospatial information and imagery.

In October, 2004, Google acquired a digital mapping company named Keyhole, Inc. Keyhole's commercially available satellite imaging software, formerly known as Earth Viewer (Albrechtslund, 2006), used satellite and aerial photography to map the surface of the earth. Soon after the acquisition of Keyhole, in March, 2005, Google introduced a free software application called Google Earth. While Google already provided a comprehensive online mapping service (Google Maps), Google Earth extended beyond the capabilities of Google Maps to include Keyhole's aerial photography of the earth's surface. Through Google Earth, users are provided with a searchable, zoomable and tiltable interface to the earth's surface and are able to annotate any location with their own bookmarks, tags and information. By using the Google Earth APP²¹, developers and programmers can create their own notational, graphical and geoinformational layers over the Earth's visual layer. And users of Google SketchUp, a free 3D modeling program, are able

²¹ API is an acronym for Application Programming Interface – APIs let applications and data 'talk' to each other in various ways. For example, a programmer might use the Google Maps API to 'plug in' GPS data from a journey around Europe in order to create a customised map of the trip, or to plot a network of hotels in Western Canada.

to design 3D models of buildings and structures, overlay them and share them via Google Earth's '3D Warehouse'.

There are also several 'informational layers' that come pre-installed in Google Earth: a 'Global Awareness' drop-down menu, which lets users choose between various social/environmental issues images and narratives provided by third parties in conjunction with Google such as 'Crisis in Darfur' presented by the United States Holocaust Memorial Museum²², or maps and images of WWF Conservation Projects. The National Geographic layer displays various points of historical and geographic interest around the globe. The application also includes several layers which map main roads and streets, terrain features, parks, shopping centres, entertainment attractions, et al.

Upon the initial release of Google Earth, as with Gmail, privacy advocates lamented the new possibilities for intrusions upon personal privacy, but this time based in visual terms rather than in informational terms, such as the ability to zoom into private property and residences from above (Albrechtslund, 2006). However, technical limitations such as the relatively limited resolution of the aerial photography and the lag time of the imagery²³ means that while users of Google Earth might be able to see the shape of a house from above, they can't peek in the windows, identify individuals or watch the inhabitants take a trip to the supermar-

²² 'Crisis in Darfur' presents an overview of the humanitarian crisis, photos and stories from refugees and victims of the crisis, maps to damaged or destroyed villages,

²³ About 1/3 of the earth is displayed at a resolution of 70cm per pixel, some countries are covered at 10cm per pixel, and the rest at 15 meters per pixel (Hankey, 2006). A 15 m resolution will show 15 meters of the Earth's surface for every pixel on your screen (a pixel is the smallest unit of measurement on a computer monitor). Imagery on Google Earth continually updated and is generally current to within 3 years (http://en.wikipedia.org/wiki/Google_Earth#Resolution_and_accuracy/).

ket in real time. Issues of national security have also been raised in relation to Google Earth: various state administrations around the world have continued to voice security-related concerns over the availability of maps of sensitive locations such as nuclear power plants, presidential residences and government facilities (Crowe, 2005). Raids on homes of suspected insurgents in Iraq have apparently yielded Google Earth print outs of British Army bases (Hung, 2007), which leads to further fears of ‘terrorists’ using Google Earth to plan and commit acts of violence. But these types of security concerns don’t seem to be valid, as studies have shown that satellite images are not detailed enough to provide potential attackers with the information necessary to conduct accurate strikes (Belopotosky, 2005).

While issues of privacy and security occupied some, many in the online community celebrated the release of the new software. By releasing Google Earth and the accompanying API, Google took information that was previously available only to commercial and private interests (those who could afford satellite imaging software or those who had security access to high resolution satellite files) and made it public and free – an important step toward Google’s ‘democratisation’ of geospatial information. Google Earth’s extensibility via the API and the ability to add and annotate customised informational layers have made it possible for various advocacy groups to easily create their own maps in order to draw attention to environmental and social concerns around the globe. Looking at Google Earth from this perspective, we can see a sort of reversal of the Panoptic gaze – where satellite imagery and mapping was previously a tool of authority and centralised surveillance, it is now available for use and rearticulation by anybody with a computer and an Internet connection.

To provide a few examples of ways in which Google Earth has been used by environmental or activist groups:

- The Sierra Club has used Google Earth to create an interactive map of the Alaskan Wildlife Reserve to protest the U.S. government's plans for oil drilling in the environmentally sensitive area ('Explore the Arctic', 2007).
- An NGO in India is using satellite images from Google Earth to counter Mumbai's attempt to set up Special Economic Zones on 10,000 hectares of village farmland. Mumbai claims that the land is infertile; the anti-SEZ group 'SEZ Hatao Sangharsh Samiti' is using imagery supplied by Google Earth to fight that claim (Tippu, 2006).
- The Surui tribe in the Amazon is working with Google to provide high resolution satellite imagery of their territory through Google Earth in order to monitor illegal loggers and miners on their 600,000 acre reserve in Brazil and also to provide an educational tool for their children by plotting points of historic and spiritual importance on the map, which leads to discussion about these locations. The Surui see this as a positive use of cultural mapping – where formerly mapping was a technique of colonisation and oppression, they are reversing the gaze of the coloniser and reclaiming indigenous identity (Garrigues, 2007).
- The Center for Public Integrity maintains an interactive map that uses the Google Maps API to plot and publicise Superfund²⁴ sites in the U.S., in an attempt to hold polluters and governments accountable for clean up efforts. The points on the map uncover responsible parties (which often includes both government institutions and

²⁴ The U.S. Federal government set up the Superfund programme in 1980 to identify the worst toxic waste sites in the country and to provide federal funds for clean up. URL: <http://www.publicintegrity.org/Superfund/report.aspx?aid=851>

corporate entities), contaminants present, action taken and progress made on each site ('Wasting Away').

Of course, while it's relatively easy to find examples of Google Earth being used in non-commercial contexts such as these and the possibilities for such 'geospatial activism' and representation will continue to be of importance, we should not neglect the massive commercial potential of Google Earth – by structuring the surface of the earth a virtualised 'site' of visual representation, advertisers and marketers are presented with a new technological canvas upon which to create new information commodities. Google has recently started testing AdWords in Google Earth by providing 'sponsored links' when searching for some locations (Meier, 2006) and as the AdWords service is propagated more fully across Google's virtual globe, businesses and organisations will have the opportunity to monetise geospatial information, not to mention the additional revenue that Google will receive from such advertising. Using Sketchup, a business could create a 3D version of its offices or branches, overlay the model in Google Earth, and purchase AdWords keywords based on geographic co-ordinates to correspond with its physical location. Enterprising companies have already started to develop large-scale advertisements that are viewable only from above: German 'land art' firm Artfield creates giant advertisements in fields and meadows for viewing both by planes and by satellites²⁵, Maxim Magazine has constructed a 'colossal babe' in the Nevada desert especially for viewing on the Google Earth ('get ready for a UFOs-eye view of gigantic hotness') (Albrechtslund, 2006), and several Target superstores in the U.S. have painted large versions of the 'Target' logo on the roof which can be seen in

²⁵ URL: <http://www.artfield.de/landart.html>

Google Earth and from planes ('Target Stores', 2005). We can expect to see many more examples of these types of advertising and branding in Google Earth as Google makes the AdWords programme more widely available and as more companies realise the productive potential of geospatial information and representations.

Google Street View²⁶ brings the surveillant gaze of Google Earth down to eye level. Google employs fleets of photographers in cars with automatic 360° cameras mounted on the roofs (White, 2007) to drive along city streets and document scenes at street level. These panoramic photographs are then digitally stitched together to provide a relatively seamless and searchable visual experience of 'walking down the middle of the road and looking around'. Cities that have been documented in this fashion (currently limited to a handful of cities in the United States) may be clicked on and browsed by anybody visiting the Google Maps site. In contrast to much of the imagery on Google Earth, however, Google Street View includes detailed and identifiable pictures of pedestrians, vehicles, buildings and structures. While taking photographs on public property is not illegal, for a company with the dataveillant capacities of Google, these all-encompassing, 360 degree view of city scenes are somewhat disturbing in their intrusiveness. There's a voyeuristic gaze in play here, as we see in articles like 'Top 15 Google Street View Sightings' (Schroeder, 2007) or sites such as 'gstreetviewsightings.com', which report on images from Google Street View – there's a man walking into an adult book shop, a man climbing up a drain pipe into an apartment (Is he breaking in? Did he lose his keys?), two women sunbathing in a park, etc.

²⁶ URL: <http://maps.google.com/help/maps/streetview/>

If we imagine that Google has plans to monetise Street View, and given Google's propensity for advertising revenue, this is not a big cognitive leap to make, Google Street View has the potential to turn photos of unknowing pedestrians into information commodities. For example, a user of Street View might be able to click on a pedestrian's piece of clothing and find the brand, the average retail cost and the cheapest place to buy it online, or the nearest shop that sells it. The pedestrian becomes a 'producing machine' in the unknowing service of informationalised capitalism.

Both Google Earth and Google Street View are unquestionably surveillant. However, an important distinction between the 'hard' panoptic gaze of CCTV and the surveillant gaze of these Google products is that CCTV is closed and institutional in nature, while Google Earth and Google Street View are available to anybody with a computer and an Internet connection. Has the surveillant gaze become 'democratised' in Google Earth and Google Street View? I would argue that the answer is at once both 'yes' and 'no'.

'Yes', because more people now have access to detailed geospatial information and imagery than ever before. This allows for many different kinds of individual and collective representations and also for the possibility of 'making power visible' through satellite imagery and customised informational layers, especially in the realm of environmental/land-based activism.

'No', because the software is 'closed source', and in contemporary capitalism, it's easy for companies to absorb dissent and even use protest and activism as a marketing/branding tool. Systems and businesses are highly flexible and can re-

flexively adjust immediately to changes in the social, cultural and commercial landscape. Alternative views are no longer excluded from consumer discourse, as we can see in the variety of activist groups using Google's products and even in the search results themselves – if one uses Google to search for 'Google sucks' or 'I hate Google', millions of results are returned. The 'socially, ethically and ecologically responsible' corporation is no longer a contradiction in terms. In fact, they've become business assets. As Michael Hardt points out, hybrid subjectivities and heterogeneity are not necessarily resistant to empire – they actually help to reinforce the locus of the market as it rules through “managing hybrid identities in flexible hierarchies” (Dumm 168). Here we can turn to the concepts of privacy and pleasure in the online consumer realm, and how these too are mobilised in the service of late capital.

VII. Privacy, Consumerism and Pleasure

“...it is important to note that social management, along whatever social trajectory, may occur even where privacy legislation or regulation exists. Indeed, the existence of privacy legislation may server to legitimate the soft social control function, by reducing public reticence about using electronic information and communication systems” (Lyons 153).

Throughout much of this enquiry, we have seen that when questions of surveillance are raised in relation to the web and Google they are often presented in terms of ‘user privacy’ or ‘security’ issues. Questions such as ‘Is personal and/or sensitive user data protected from unauthorised access by third parties such as advertisers, government authorities and crackers? When a user signs up for a web service such as Gmail or purchases goods from Amazon.com, how do they know that their personal e-mails and credit card information remain safe and secure? Can people remain anonymous when using search engines, e-mail programmes and other web applications?’ Most websites have privacy policies in place to address these sorts of concerns. Privacy policies are detailed documents which outline what kinds of information are collected about users²⁷, how that information is used by the company and who it might or might not be shared with. While Google’s services are often a focus of privacy advocacy groups due to its size and market dominance, the company is nonetheless frequently cited positively for its principled

²⁷ On a technical level, things like IP address, browser and computing platform used, where the user is coming from, how long they spend on the page, what parts of the page are clicked on, etc; on a personal level, information such as e-mail address, age, name, country, phone number, etc.

stance on privacy and its refusal to share user information and search histories with government entities²⁸.

However, Google (along with other online companies) has no financial incentive to violate its users' privacy. Google doesn't have a vested interest in selling user information to marketing companies or giving information to government agencies, because it can make more money and maintain a strong brand image by keeping user information private and secure. Securing and maintaining user privacy is a business asset for online companies, not a liability – especially for Google, the company with a 'divine' soul²⁹. Indeed, as David Lyons notes in the above quote, perhaps by focussing so much attention on online 'privacy', the question of *control* and how it is distributed doesn't receive much consideration in studies of online surveillance. Perhaps the existence of privacy policies and legislation actually serves to mask the deeper ideological function of information surveillance – that is, to articulate consumers within a specific target demographic. Once we are assured of our privacy, then we are 'free' to act and consume as we wish. This notion of consumer 'freedom' assured by 'privacy' marks an important shift in the production of social management and control: from repression to seduction, from discipline to pleasure. Whereas self-assertion and methods of social integration were previously manifested in modes of production and sites of control such as the

²⁸ In August, 2006, the US Justice Department issued a request to Google, AOL, Yahoo, and MSN for millions of search queries as part of a court case related to online pornography laws. Only Google refused, citing that the request was "unnecessary, overly broad, would jeopardize trade secrets, and expose identifying information about its users" (Hafner).

²⁹ "We consider ourselves a company that does no evil, and we take user privacy seriously...We have very strict internal rules, even among Google employees who are able to access confidential data. It would harm Google enormously, if we behaved badly with personal data. I don't believe we ever will" (McCullagh).

work-place and the church, they are now tied to freedom of choice in the global marketplace. In 'Freedom', Zygmunt Bauman interrogates the history of the social relation of 'freedom' as it moved from the sphere of work into the sphere of consumerism. For Bauman, freedom is a social relation and 'free agents' are produced according to the dictates of power in any certain historical period. In the current period of late capitalism, freedom is defined by the ability of the individual to choose goods and services without hindrance. As Bauman notes,

“The production of consensus and the solicitation of appropriate social conduct are taken care of by the consumer market...The market orientation of individuals pursuing the satisfaction of their ever-rising needs is all that is needed for social integration” (81).

Bauman's view is very similar to that position taken by Hardt and Negri in 'Empire' – that is, control is exercised through the communicative networks of global capitalism, and that “behaviours of social integration and exclusion proper to rule are thus increasingly interiorized within the subjects themselves” (23). The attraction of the shiny, pleasurable consumer lifestyle is how capitalism perpetuates itself and 'soft' surveillance works in service of this perpetuation. Far from suppressing desire and individual freedom, reproduction of the capitalist system is realised by fulfilling these subjectivities. A plurality of views, lifestyles, beliefs and behaviours may be practised within this framework – heterogeneity is no longer a threat but an opportunity for new markets to develop and new needs to be created.

We can see this approach to 'consumer freedom' reflected in the rhetoric of Google – in their desire to fulfil 'wants' and 'needs', to provide relevant advertise-

ments that are ‘good and useful for the consumer’, to build a platform that mediates worldwide information supply and demand, to ‘democratise’ access to all types of information. It’s in Google’s interest to increase diversity and hybridity in their user base and in use of their products, as the broader the user base, the wider the economic net. In choosing to use Google’s products, however useful, relevant or democratic they may be, users are subject to the discourse of informational capitalism. However, since this discourse is pleasurable and useful, most individuals are willing participants. Indeed, surveillance itself can be a seductive and enjoyable part of mediated consumer society, as Joseph Krandall points out in ‘Operational Media’:

“In media-saturated societies, surveillance has gradually been made ‘friendly’ and transformed into spectacle, to the extent that it is no longer a condition to be feared. Rather, it is a condition to be courted: witness the phenomena of reality television, blogs, and webcams, and the rise of the media *mise-en-scene* as the primary form of social authentication” (Krandall).

Now that systems of control throughout the network society are pleasurable and consumer based, it might appear that all online activity would be subsumed under the banner of consumerism. But is online surveillance rooted in informationalised consumer society as totalised as this enquiry has thus far indicated? I don’t believe so, and in the next chapter and in my conclusion, I will summarise several of the myriad ways in which online surveillance can be resisted, contested and even turned back on itself.

VIII. Resisting the Panoptic Gaze

“These gazes cannot all be said to be subsumed to an overarching capitalist gaze simply because they exist in a medium created by and permeated by consumerism whose hardware relegates some to the center and others to the periphery. The consumerist tendency is panoptic, but the working out of the gaze is as yet too heterogeneous to be considered appropriated”

David Winokur, ‘The Ambiguous Panopticon’

To take a utopian view of the Net as a decentralised, democratic information commons open to all and ideologically neutral is obviously misguided. We have seen throughout this enquiry the various ways in which the discourse of consumerism pervades many aspects of online activity through surveillance, commodification and pleasure. However, to take the totalised, dystopian view in which *all* online behaviour is subject to a commercialising gaze and politics foreclosed upon is perhaps just as ill-considered. Communication networks and peer-to-peer technologies also give individuals and groups the opportunity to organise, communicate, distribute and publish a wide variety of material across disparate boundaries to a larger audience than was traditionally possible with expensive print media. Additionally, surveillance is not simply a top-down or centre-out phenomenon – technologies can be used to return or resist the ‘gaze of the surveyor’ in some cases. To subvert panoptic power, the ‘prisoners’ must be able to watch the ‘guards’.

For example, when anonymous users were found to be editing entries somewhat nefariously on the collective encyclopedia Wikipedia, Virgil Griffith, a researcher at the California Institute of Technology, built an online application

called the Wikiscanner³⁰ which allows specific edits to be compared with corresponding IP addresses. Among the many edits found using Wikiscanner: workers operating from CIA computers have been caught editing entries about Richard Nixon and Ronald Reagan, IP addresses from Fox News headquarters have edited out negative comments related to Fox News³¹, and a computer in Democratic party headquarters was used to edit a page about conservative talk show host Rush Limbaugh, calling him ‘idiotic’ and ‘ridiculous’ (Johnson, 2007).

There are many other examples of free and open-source software projects that are attempting to build alternatives to the commercialised, closed-source environments which currently dominate much of the mainstream web:

- Openstreetmap.org is a grassroots effort to map cities and spaces around the world with GPS and GIS systems, human volunteers and open source technologies³². While Google Maps and Google Earth have APIs which allow developers to ‘interact’ with the data, the source code itself is closed. OpenStreetMap is open source, which means that any person is free to view, re-use and update the data in a collaborative manner.
- The free and open source media player Miro (formerly known as the Democracy Player), produced by the Participatory Culture Foundation³³, allows individuals

³⁰ URL: <http://wikiscanner.virgil.gr/>

³¹ URL: <http://wired.reddit.com/wikidgame/>

³² URL: <http://www.openstreetmap.org>

³³ URL: <http://participatoryculture.org/>

and groups to produce and distribute video feeds independently of advertising, mainstream distributors and media companies.

- Open source web browsers such as Mozilla Firefox and Camino can incorporate software plugins such as Adblock³⁴ which block most Internet advertising, both text-based and graphical, as one surfs the web.
- Search Wikia is an open source search engine currently in the development and planning phase. Search Wikia's 4 organising principles are worth noting here:
 1. Transparency - Openness in how the systems and algorithms operate, both in the form of open source licenses and open content + APIs.
 2. Community - Everyone is able to contribute in some way (as individuals or entire organizations), strong social and community focus.
 3. Quality - Significantly improve the relevancy and accuracy of search results and the searching experience.
 4. Privacy - Must be protected, do not store or transmit any identifying data.³⁵

In marked contrast to the closed algorithms and data storage of Google, Search Wikia is based around openness and transparency. It will be interesting to see how this technology develops, and if it is able to scale in size without the massive commercial revenue of Google.

³⁴ URL: <https://addons.mozilla.org/en-US/firefox/addon/10>

³⁵ URL: http://search.wikia.com/wiki/Search_Wikia

There are also many media artists³⁶ critically engaging with issues of surveillance and control in society – Steve Mann’s wearable surveillance cameras³⁷, Christian Nord’s GPS/Google Earth BioMapping³⁸ project, and Mongrel’s ‘Video Sniffin’ piece, which sniffs out wireless CCTV networks and ‘reclaims’ them for art and music projects with young people³⁹.

These various projects show that we shouldn’t neglect the idea of agency in the face of pervasive surveillance. While technological utopianism isn’t a viable solution to problems of surveillance, neither is deep pessimism. In my conclusion, I continue this line of thought and present further possibilities for educating web users about issues of surveillance online.

³⁶ For a more comprehensive list of media artists working with surveillance, see Ctrl Space by Levin, et al.

³⁷ URL: <http://www.wearcam.org/>

³⁸ URL: <http://www.biomapping.net/>

³⁹ URL: <http://www.mongrelx.org/?q=videosniffin>

IX. Conclusion

As David Lyons notes in ‘The Electronic Eye’, surveillance is “neither overwhelmingly negative in its effects nor incorrigibly evil in its character” (223). Indeed, one could say the same thing about Google. While the company’s totalising mission certainly raises issues of power and control in information surveillance and we find its business practices firmly rooted within the dominant discourse of consumer capitalism, the company’s search engine and various software products also provide a beneficial service for many web users and people seeking information around the world – not just those seeking to purchase products or build businesses. To distil Google down to an ‘Evil Consumerist Panopticon’ would be a vast oversimplification of the heterogeneous ways to which its diffuse services can be put to use.

However, it’s precisely the pervasiveness of this type of ‘soft’ surveillance which makes a critical awareness of the issues surrounding it necessary. ‘Hard’ technologies such as CCTV or national ID cards make common targets for popular surveillance commentary, but the more distributed, pleasurable nodes of surveillance on the web are more difficult to survey and place. Surveillance is always a method of exercising power in some way, a technique of control, and it is here where we need to take a sceptical but informed approach to the ways in which surveillance is manifested online. Perhaps a practical starting point would be to better educate web users and students about issues of online surveillance: how to deal with and delete cookies, how to critically read privacy policies, the availability of high quality open source and free software, when not to provide personal information to websites, how to create websites and publish independently, etc.

I believe that it's possible to adopt a non-totalising and non-binary stance regarding surveillance, power, capital and control on the web. Just as there are spaces of resistance and zones of autonomy within earlier communication media (i.e. pirate and independent radio, independent zines, books, films and music), so will there continue to be people and groups struggling to reclaim and reterritorialise discourses of power in the decentralised communication networks of informationalised capital – and these sorts of activities don't necessarily exclude utilising commercial technologies such as Google Earth or social networking websites. A conscious and creative awareness of these issues can help us to engage critically with forms of surveillant power and aid in the articulation of alternative and resistant discourses wherever possible.

X. Bibliography

- Albrechtslund, Anders. 'Surveillance in Searching.' August, 2006.
<<http://www.albrechtslund.net/wordpress/wp-content/uploads/2006/08/Surveillanceinsearching1.pdf>> (accessed June 20, 2006).
- Allen, Katie. 'CBS buys Last.fm in largest UK web 2.0 acquisition to date.'
Guardian Unlimited. May 30, 2007.
<<http://business.guardian.co.uk/story/0,,2091412,00.html>>
(accessed 2 September 2007).
- Arrington, Michael. 'A Comparison of Live Hotmail, Gmail and Yahoo Mail.'
Tech Crunch. February 8, 2007.
<<http://www.techcrunch.com/2007/02/08/a-comparison-of-live-hotmail-gmail-and-yahoo-mail>> (accessed 4 August 2007)
- Armstrong, Heather. 'Collecting Unemployment.' Dooce.com. February 26, 2002.
<http://www.dooce.com/archives/daily/02_26_2002.html>.
(accessed 14 August 2007).
- Battelle, John. The Search. London: Nicholas Brealey, 2005.
- Bauman, Zygmunt. Freedom. Milton Keynes: Open University, 1988.
- Belopotosky, Danielle. 'Google satellite imaging software raises terrorism concerns.'
National Journal's Technology Daily. August 25, 2005.
<<http://www.govexec.com/dailyfed/0805/082405td2.htm>>
(accessed 3 August 2007).

Blanco, Leo. 'Gmail removes invitation restrictions.' TMCnet. February 15, 2007.

<<http://www.tmcnet.com/news/2007/02/15/2340298.htm>>

(accessed 4 August 2007).

Coombes, Andrea. 'Worker email increasingly monitored, used in court.'

Marketwatch. July 30, 2007. <<http://tinyurl.com/2rl7vm>> (accessed

August 2007).

Crowe, Jonathan. 'Google Earth Privacy and Security Roundup.' The Map Room.

<http://www.mcwetboy.net/maproom/2005/09/google_earth_pr_1.php>

(accessed 31 August 2007).

Dean, Jodi. 'The Networked Empire: Communicative Capitalism and the Hope for Politics.' Empire's New Clothes: Reading Hardt and Negri.

Passavant, Paul & Jodi Dean, eds. New York: Routledge, 2004.

Deleuze, Gilles. 'Postscript on Control Societies.' Ctrl Space: Rhetorics of Surveil-

lance from Bentham to Big Brother. Levin, Thomas Y., Ursula Frohne, and

Peter Weibel, eds. Cambridge, Mass: MIT Press, 2002.

'Digital Dirt Derails More Job Searches, As Recruiters' Use Of Search Engines Increases.' Execunet. August 16, 2007.

<http://www.execunet.com/m_releases_content.cfm?id=3651>

(accessed 2 September 2007).

Dumm, Thomas L. 'Sovereignty, Multitudes, Absolute Democracy: A Discussion between Michael Hardt and Thomas L. Dumm about Hardt's and Negri's Empire.' Empire's New Clothes: Reading Hardt and Negri.

Passavant, Paul & Jodi Dean, eds. New York: Routledge, 2004.

'Explore the Arctic.' Arctic National Wildlife Refuge.

<<http://www.sierraclub.org/arctic/maps/>> (accessed 20 August 2007).

'Fiscal Year 2006 Results.' January 31, 2007.

<<http://investor.google.com/releases/2006Q4.html>> (accessed 14 August 2007).

Foucault, Michel. Discipline and Punish. London: Penguin, 1977.

Garrigues, Lisa. 'Surui partner with Google Earth to map territory.'

Indian Country Today. July 2, 2007.

<<http://www.indiancountry.com/content.cfm?id=1096415314>> (accessed 20 August 2007).

Hafner, Katie and Matt Richtel. 'Google Resists U.S. Subpoena of Search Data.'

The New York Times. January 20, 2006.

<<http://www.nytimes.com/2006/01/20/technology/20google.html?ex=1189137600&en=a4f43dab6394eed9&ei=5070>> (accessed 29 August 2007).

Hanke, John. 'Happy Birthday Google Earth.' The Official Google Blog.

June 12, 2006. <<http://googleblog.blogspot.com/2006/06/happy-birthday-google-earth.html>> (accessed 1 August 2007).

Hardt, Michael and Anotonio Negri. Empire. Cambridge, Mass: Harvard, 2000.

Hu, Jim. 'Yahoo buys photo-sharing site Flickr.' Cnet News. March 20, 2005.

<http://news.com.com/Yahoo+buys+photo-sharing+site+Flickr/2100-1038_3-5627640.html> (accessed 2 September 2007).

Hung, Tony. 'Terrorists Using Google Earth to Pinpoint Attacks.' Blog Herald.

January 15, 2007. <<http://www.blogherald.com/2007/01/15/terrorists-using-google-earth-to-pinpoint-attacks/>>

(accessed 26 August 2007).

'IAB Internet Advertising Report - Full year 2006.' Interactive Advertising Bureau.

May, 2007. FILE.

'IMF Report for Selected Countries and Subjects.' World Economic Outlook

Database. April 2007. <<http://tinyurl.com/33ofbm>> (accessed 7 August 2007).

Jarboe, Greg. 'Stats Show Google Dominates the International Search Landscape.'

Searchenginewatch.com. February 22, 2007.

<<http://searchenginewatch.com/showPage.html?page=3625072>>

(accessed 7 August 2007).

Johnson, Bobbie. 'Companies and party aides cast censorious eye over Wikipedia.'

The Guardian. August 15, 2007.

<<http://www.guardian.co.uk/technology/2007/aug/15/wikipedia.corporateaccountability?gusrc=rss&feed=networkfront>>

(accessed 26 August 2007).

- Kinnier, Alex. 'Why We're Buying DoubleClick.' The Official Google Blog. June 26, 2007. <<http://googleblog.blogspot.com/2007/06/why-were-buying-doubleclick.html>> (accessed 14 August 2007).
- Krandall, Joseph. 'Operational Media.' CTheory.net. January 6, 2005. <<http://www.ctheory.net/articles.aspx?id=441>> (accessed 20 June 2007).
- 'Leading Search Engines.' Hitwise. July, 2007. <<http://www.hitwise.com/datacenter/searchengineanalysis.php>> (accessed 7 August 2007).
- Levin, Thomas Y., Ursula Frohne, and Peter Weibel, eds. Ctrl Space: Rhetorics of Surveillance from Bentham to Big Brother. Cambridge, Mass: MIT Press, 2002.
- Lyons, David. The Electronic Eye: The Rise of Surveillance Society. Cambridge: Blackwell, 1994.
- Manovich, Lev. 'Modern Surveillance Machines: Perspective, Radar, 3-D Computer Graphics, and Computer Vision.' Ctrl Space: Rhetorics of Surveillance from Bentham to Big Brother. Levin, Thomas Y., Ursula Frohne, and Peter Weibel, eds. Cambridge, Mass: MIT Press, 2002.
- McCahill, Michael and Clive Norris. 'CCTV in London.' Urban Eye. June, 2002.
- McCullagh, Declan. 'Is Google the future of e-mail?' Cnet News. April 12, 2004. <<http://news.com.com/2010-1032-5187543.html>> (accessed 2 August 2007).

- Meier, Reto. 'Google Earth Showing Sponsored Links.' The Radioactive Yak. May 8, 2006. <<http://blog.radioactiveyak.com/2006/05/google-earth-showing-sponsored-links.html>> (accessed September 1 2007).
- Nussbaum, Emily. "Say Everything." New York Magazine. February 12, 2007. 24-29, 102-103.
- Quinton, Brian. 'Study: Users Don't Understand, Can't Delete Cookies.' Directmag.com. May 18, 2005. <http://searchlineinfo.com/InsightExpress_cookie_study/> (accessed 14 August 2007).
- Schmidt-Burkhardt, Astrit. 'The All-Seer: God's Eye as Proto-Surveillance.' Ctrl Space: Rhetorics of Surveillance from Bentham to Big Brother. Levin, Thomas Y., Ursula Frohne, and Peter Weibel, eds. Cambridge, Mass: MIT Press, 2002.
- Schroeder, Stan. 'Top 15 Google Street View Sightings.' Mashable. May 15, 2007. <<http://mashable.com/2007/05/31/top-15-google-street-view-sightings/>> (accessed 26 August 2007).
- 'Search Engine Market Score.' comScore Data Center. July, 2007. <<http://www.comscore.com/press/data.asp>> (accessed 4 August 2007).
- Shapiro, Kam. 'The Myth of the Multitude.' Empire's New Clothes: Reading Hardt and Negri. Passavant, Paul & Jodi Dean, eds. New York: Routledge, 2004.
- Shodjai, Payam. 'Your slice of the web.' The Official Google Blog. April 19, 2007.

<<http://googleblog.blogspot.com/2007/04/your-slice-of-web.html>>

(accessed 26 August 2007).

Siklos, Richard. 'News Corp. to Acquire Owner of MySpace.com.' The New York Times. July 18, 2005. <<http://tinyurl.com/3dj9ld>> (accessed 9 August 2007).

Tippu, Sufia. 'Google Earth to Save Villages.' IT Wire. October 19, 2006.

<<http://www.itwire.com/content/view/6465/>> (accessed 19 August 2007).

Thompson, Clive. 'Open Source Spying.' The New York Times. December 3, 2006.

<<http://tinyurl.com/2taf9d>> (accessed 4 August 2007).

'Wasting Away.' The Center for Public Integrity.

<<http://www.publicintegrity.org/Superfund/>> (accessed 23 August 2007).

Waters, Darren. 'Pick of the blogs: Dooce.' BBC News. July 20, 2005.

<<http://news.bbc.co.uk/1/hi/entertainment/4659469.stm#dooce>>

(accessed 7 August 2007).

White, Charlie. 'Google Streetview Camera Car Fleet Set to Invade America.'

Gizmodo. July 17, 2007. <<http://gizmodo.com/gadgets/eye-on-you/google-streetview-camera-car-fleet-set-to-invade-america-279222.php>>

(accessed 26 August 2007).

Willison, Simon. 'The Mind of God.' July 18, 2006.

<<http://simonwillison.net/2002/Jul/28/theMindOfGod/>>

(accessed 6 August 2007).

Winokur, Mark. 'The Ambiguous Panopticon: Foucault and the Codes of Cyberspace.' CTheory.net. January 13, 2003.
<<http://www.ctheory.net/articles.aspx?id=371>> (accessed 20 June 2007).