

Chapter 1 : Michel Foucault: Disciplinary Power: Panopticism

Self-surveillance / government, mobile, privacy Just because there's no content that comes with the metadata doesn't make the latter useless. Using Amazon's \$5 button for personal data collection.

Our choices often reflect how we feel and vice versa, so it is only natural that there are personal trackers to monitor mental health, or more specifically, our emotions. Developers are challenged with the quantification of something that is innately non-numeric. What numeric value do we put on happy, sad or something in between? A few applications, while not perfect, have attempted to measure and visualize the complexity of human emotion. Moodstats [12] and Lifemetric [13] use a collection of sliders and gauges to let users put numeric values on their emotions. Moodstats looks and works a lot like a sound equalizer. Move the switches up and down for mood, stress levels and creativity along with some non-emotional metrics like number of emails sent, exercise and achievements. Users can also enter diary entries, which is really a form of annotation. As the user looks at past emotions, the diary can be used to make inferences about what causes certain levels of mood. Lifemetric is similar but also applies a social aspect to self-surveillance. Users move a scroll bar all the way left if they are sad and to the far right if they are happy and then anything in between. On any given day, users not only see how they feel, but also how the rest of the Lifemetric community feels. Self-surveillance does not always have to be aimed inward. Sometimes it can be aimed outwards to the relationships we have with our surroundings. We have a give-and-take relationship with our environment that we are not always aware of. What quantity of natural resources do we consume, how much energy do we use and what effects do we have on the environment? The answers come back to the tiny choices we make every day. Do we turn the lights off when we leave a room? Do we combine driving trips to reduce travel time? These questions can go unanswered even though they can collectively have a huge impact on the environment. PEIR allows users, based on their travel patterns, to see how they personally affect the environment in terms of carbon impact and particulate matter exposure. Users collect GPS data with their mobile phones, and PEIR processes the data using established micro-environment models to show users how they affect the environment and how the environment affects them. To a similar end WattzOn [15] uses a detailed questionnaire to estimate energy consumption. Users answer questions like how many times they fly per year on average and what kind of car they drive. Results can then be compared against others and national averages for context. Perhaps the main point so far is that if you want to track something about your life, there is probably an application that will help you do it. Me-trics [16], Daytum [17] and Your. Some data streams are automatically logged, like number of bookmarks to the social bookmarking site delicious. These generalized self-surveillance tools bring several data streams into a single location, which makes it much easier to infer patterns and outliers. The reader should notice that all the mentioned applications use visualization to present users their data. Visualization helps users, who are not necessarily data professionals, interpret their data and hopefully make educated decisions based on what they see. As a result, visualization designers have a responsibility to communicate personal data clearly in the same way that journalists have to report the news accurately. As data collection and visualization advance and users become more comfortable with data, personal data collection could become common practice. Our credit card bills and bank statements can be accessed online; web browsing and Google searches are stored in data logs; and grocery stores keep track of products we purchase. All these data are passive in that users do not have to actively collect it. On the flip side, there are a number of tools that let users play an active role. While these tools are specifically designed for data collection and analysis, we can also add mobile phones to the list. It is easy to see how we can repurpose devices as personal sensors. As data collection has advanced and different streams of different data types have developed, so have the visualizations. Visualization has moved from static bar graphs and dot plots to interactive and animated visualizations. These changes, of course, have not always been for the better, but when done right, these new formats allow users to explore their data and see patterns without any formal training in analysis. Tools like Processing [22] and Flash [23] have grown more robust so that developers have more options available to them, and as a result, those who have data, have more opportunity to visualize

and make inferences. We also see a trend in collaborations between art and science to make visualization both scientifically accurate and emotionally engaging. Works from groups like Stamen Design [25] and designers like Jonathan Harris [26] are quickly bridging the gap between design and statistics. Such works encourage users to dig deeper and attract those who once looked at data with a skeptical eye. Data visualization can advance all it wants to, but not much is gained if users are not comfortable with the interface. However, we can see many examples of good design on the web. Stamen Design constantly preaches data visualization as interface and has seen much success in collaborations with sites like Digg [31] and Twitter. In September the Times graphics department produced a tree map to show market loss by major companies [32]. In August they published a weighted network graph that showed Olympic medal counts by country and year [33]. Tree map showing A Year of Heavy Losses [www](#).

Chapter 2 : (Self-)Surveillance, Anti-Doping, and Health in Non-Elite Road Running

I did all of this using gadgets that point toward a time when complete self-surveillance will be the norm. My goal of experimenting with personal data and attempting to self-experiment by living just a little bit in the future was easier than I thought.

The computers running the database are contained in an underground facility about the size of two American football fields. Surveillance aircraft Micro Air Vehicle with attached surveillance camera Aerial surveillance is the gathering of surveillance, usually visual imagery or video, from an airborne vehicle—such as an unmanned aerial vehicle, helicopter, or spy plane. Military surveillance aircraft use a range of sensors e. Digital imaging technology, miniaturized computers, and numerous other technological advances over the past decade have contributed to rapid advances in aerial surveillance hardware such as micro-aerial vehicles, forward-looking infrared, and high-resolution imagery capable of identifying objects at extremely long distances. For instance, the MQ-9 Reaper, [87] a U. They have developed systems consisting of large teams drone planes that pilot themselves, automatically decide who is "suspicious" and how to go about monitoring them, coordinate their activities with other drones nearby, and notify human operators if something suspicious is occurring. This greatly increases the amount of area that can be continuously monitored, while reducing the number of human operators required. Thus a swarm of automated, self-directing drones can automatically patrol a city and track suspicious individuals, reporting their activities back to a centralized monitoring station. Data profiling can be an extremely powerful tool for psychological and social network analysis. A skilled analyst can discover facts about a person that they might not even be consciously aware of themselves. In the past, this data was documented in paper records, leaving a "paper trail", or was simply not documented at all. Correlation of paper-based records was a laborious process—it required human intelligence operators to manually dig through documents, which was time-consuming and incomplete, at best. But today many of these records are electronic, resulting in an "electronic trail". Every use of a bank machine, payment by credit card, use of a phone card, call from home, checked out library book, rented video, or otherwise complete recorded transaction generates an electronic record. Public records—such as birth, court, tax and other records—are increasingly being digitized and made available online. In addition, due to laws like CALEA, web traffic and online purchases are also available for profiling. Electronic record-keeping makes data easily collectable, storable, and accessible—so that high-volume, efficient aggregation and analysis is possible at significantly lower costs. Information relating to many of these individual transactions is often easily available because it is generally not guarded in isolation, since the information, such as the title of a movie a person has rented, might not seem sensitive. However, when many such transactions are aggregated they can be used to assemble a detailed profile revealing the actions, habits, beliefs, locations frequented, social connections, and preferences of the individual. The centers will collect and analyze vast amounts of data on U. Miller, data held by third parties is generally not subject to Fourth Amendment warrant requirements. The data collected is most often used for marketing purposes or sold to other corporations, but is also regularly shared with government agencies. Although there is a common belief that monitoring can increase productivity, it can also create consequences such as increasing chances of deviant behavior and creating punishments that are not equitable to their actions. It can be used for direct marketing purposes, such as targeted advertisements on Google and Yahoo. These ads are tailored to the individual user of the search engine by analyzing their search history and emails [] if they use free webmail services, which is kept in a database. An IP address and the search phrase used are stored in a database for up to 18 months. Their revenue model is based on receiving payments from advertisers for each page-visit resulting from a visitor clicking on a Google AdWords ad, hosted either on a Google service or a third-party website. This information, along with the information from their email accounts, and search engine histories, is stored by Google to use for building a profile of the user to deliver better-targeted advertising. In addition, most companies use software to block non-work related websites such as sexual or pornographic sites, game sites, social networking sites, entertainment sites, shopping sites, and sport sites. The American Management Association and the ePolicy Institute also stress

that companies "tracking content, keystrokes, and time spent at the keyboard The Department of Homeland Security has openly stated that it uses data collected from consumer credit and direct marketing agencies" such as Google" for augmenting the profiles of individuals whom it is monitoring. Nevertheless, human infiltrators are still common today. For instance, in documents surfaced showing that the FBI was planning to field a total of 15, undercover agents and informants in response to an anti-terrorism directive sent out by George W. Reconnaissance satellite On May 25, the U. Director of National Intelligence Michael McConnell authorized the National Applications Office NAO of the Department of Homeland Security to allow local, state, and domestic Federal agencies to access imagery from military intelligence Reconnaissance satellites and Reconnaissance aircraft sensors which can now be used to observe the activities of U. The satellites and aircraft sensors will be able to penetrate cloud cover, detect chemical traces, and identify objects in buildings and "underground bunkers", and will provide real-time video at much higher resolutions than the still-images produced by programs such as Google Earth. Some nations have an identity card system to aid identification, whilst others are considering it but face public opposition. In this case it may create an electronic trail when it is checked and scanned, which can be used in profiling, as mentioned above. RFID and geolocation devices[edit] Hand with planned insertion point for Verichip device RFID tagging[edit] Radio Frequency Identification RFID tagging is the use of very small electronic devices called "RFID tags" which are applied to or incorporated into a product, animal, or person for the purpose of identification and tracking using radio waves. The tags can be read from several meters away. They are extremely inexpensive, costing a few cents per piece, so they can be inserted into many types of everyday products without significantly increasing the price, and can be used to track and identify these objects for a variety of purposes. Verichip is slightly larger than a grain of rice, and is injected under the skin. The injection reportedly feels similar to receiving a shot. The chip is encased in glass, and stores a "VeriChip Subscriber Number" which the scanner uses to access their personal information, via the Internet, from Verichip Inc. Thousands of people have already had them inserted. This information could be used for identification, tracking, or targeted marketing. As of [update] , this has largely not come to pass. GPS tracking In the U. The geographical location of a mobile phone and thus the person carrying it can be determined easily whether it is being used or not , using a technique known multilateration to calculate the differences in time for a signal to travel from the cell phone to each of several cell towers near the owner of the phone. Victor Kappeler [] of Eastern Kentucky University indicates that police surveillance is a strong concern, stating the following statistics from Of the , law enforcement requests made to Verizon, 54, of these requests were for "content" or "location" information" not just cell phone numbers or IP addresses. Content information included the actual text of messages, emails and the wiretapping of voice or messaging content in real-time. A comparatively new off-the-shelf surveillance device is an IMSI-catcher , a telephone eavesdropping device used to intercept mobile phone traffic and track the movement of mobile phone users. IMSI-catchers are used in some countries by law enforcement and intelligence agencies , but their use has raised significant civil liberty and privacy concerns and is strictly regulated in some countries. Microchip implant human A human microchip implant is an identifying integrated circuit device or RFID transponder encased in silicate glass and implanted in the body of a human being. A subdermal implant typically contains a unique ID number that can be linked to information contained in an external database, such as personal identification, medical history, medications, allergies, and contact information. Several types of microchips have been developed in order to control and monitor certain types of people, such as criminals, political figures and spies,[clarification needed] a "killer" tracking chip patent was filed at the German Patent and Trademark Office DPMA around May

Chapter 3 : Computer and network surveillance - Wikipedia

electronic surveillance - surveillance by electronic means (e.g. television) *vigil, watch* - a purposeful surveillance to guard or observe *stakeout* - surveillance of some place or some person by the police (as in anticipation of a crime).

Advanced Search Histories of late nineteenth- and early twentieth-century medicine emphasise the rise of professional and scientific authority, and suggest a decline in domestic health initiatives. Exploring the example of weight management in Britain, we argue that domestic agency persisted and that new regimes of measurement and weighing were adapted to personal and familial preferences as they entered the household. Taking one case study—the management and measurement of weight—our article explores nineteenth- and twentieth-century persistence, and even expansion, of domestic agency and activity in the pursuit of health. We examine the myriad new forms of information, techniques and devices created and marketed specifically for household use as a way to access householders themselves, who often remain silent in the historical record. Together with the more fragmentary direct evidence available about users and choosers in the home, these sources generate a picture of British homes as vibrant sites of health agency and medical decision taking. Such close scrutiny illuminates the diverse ways in which nineteenth- and twentieth-century householders acquired and responded to information on the regulation of food intake and the relationship between weight, health and physical appearance. Focusing on the under-studied British context but informed by the rich literature on US weight management, our analysis interrogates the sources of information available to householders on weight and its management. Did the advent of particular models of surveillance—in particular, the gradual rise of domestic technologies of exact measurement—have any impact on domestic agency? Were patients, consumers and health seekers empowered by increased access to the tools of professional medicine here, advice on diet, dietary tables and scales, or colonised by them? Our article commences with a discussion of the contribution of household guides to health in offering advice and guidance on the management of weight in the home. We explore how mechanistic approaches of self-surveillance were absorbed into a literature that already extolled moderate food intake, encouraged householders to take responsibility for weight management, and instructed them in the skills of exact measurement. After briefly introducing the rise and especially the commercial diffusion of quantitative approaches to health—and with them, the emergence of normative responses to weight variation—we turn to the role of the adult personal scales in particular. Health Guides and Weight Monitoring in the Nineteenth-century Home Excessive weight has long attracted medical and lay attention; notable figures of vast girth and bulk generated public fascination, derision, mirth and admiration while their expanding waistlines were described and illustrated in paintings, novels, pamphlets and the press. By the mid-nineteenth century, hydropathy, with its rigorous regimes of cold water treatments, pummelling and massage, temperate diet and open-air exercise, reproved the moral failings of overindulgence while treating its physical effects. Meanwhile, dietary guides and public weighing serviced an increasing fascination with measuring weight and moderating it. The emergence of new fat fighting products intersected with fashion for thinness, media interest in dieting, and the production of insurance tables proclaiming norms of height and weight. How did families acquire and act upon information about weight loss or gain and nutrition more generally? Did they call in medical assistance to deal with weight gain or tackle it themselves? Household medical guides illustrate the ways in which diet and attention to weight were introduced to the nineteenth-century home. The growth in the number of such publications and their frequent re-publication in large print runs testifies to the strong market for such guides, as part of a wider expansion of advice literature targeted at families. Advocates of new healing approaches, including the nineteenth-century systems of hydropathy, homoeopathy, medical botany and vegetarianism, meanwhile, infused their attempts to empower families with knowledge and technical skills with a missionary zeal, encouraging them to actively treat a variety of medical disorders and to initiate interventions to improve their general health and well-being. To reduce fat, Gardner recommended active exercise, lowered starch consumption, avoidance of sugar and wine and the substitution of bread with thin, browned toast and hard biscuits. Health guides produced by advocates of new medical systems were equally unambiguous about the responsibility borne by individuals and

householders in managing health, and concluded that gluttony produced poor health and illustrated moral weakness. Such texts offered guidance on eating as moral education, whereby the stomach was to be ruled by the head and regimes of moderation and regularity encouraged. Healthy living meant living naturally. For the Olsens and many other writers on health bodily size was to be restrained largely through the regulation of behaviour and emotion in response to environmental and cultural cues, rather than those supplied by the actual measurement of girth and weight. By the late nineteenth century, health advice was becoming ever more specialised. Guides catered for discrete audiences and no more so than for women and girls, many of whom were interested in regulating body weight for reasons of beauty and fashion as much as health. Health advice handbooks, health periodicals and magazines for women and girls elaborated increasingly on the ways and means of controlling weight, improving the figure and developing correct proportions. Instead, she was urged to become an early riser, to take brisk walks and exercise and to consume uncooked fruits, vegetables, white fish, lemon tea and rusks while avoiding farinaceous dishes, milk, sweets, pastry, cocoa and alcohol. In other words it stands ready to destroy both health and beauty. The widely-perceived need for weight control remained only one part of a wider agenda of domestic management of the self. Close self-scrutiny and attentive self-surveillance were essential to both sides of this equation for health maintenance. Enumerating the Normal In general, nineteenth-century health guides intended for the household reader did not yet emphasise surveillance by numbers. Not until the end of the century would they include straightforward tables relating ideal weight to gender, height, physical development, occupation and exercise, and cite hospital dietaries or diet tables drawn up by physicians as useful guides to what individuals should eat. They introduced householders to a wide array of measuring paraphernalia from graduated wine glasses, funnels and measures to scales and weights for manufacturing and dispensing remedies, encouraging the adoption of practices of exact measurement. Moreover, sensory data, if captured only in words could not be minutely compared between practitioners or cases. In contrast, the new measuring instruments could provide exactly the definitive information required in the form of a numerical reading, readily comparable to similar readings taken for other patients. Hutchinson lauded the advantages offered to the medical professional by all such technological aids: The rise of quantification in clinical practice required both the organised and systematic collection of the individual measurements of numerous individuals, and the correlation of those numbers with other quanta of embodiment: Speaking directly to his peers in the growing insurance industries of Britain and the United States, Hutchinson extolled weight as the most reliable predictor of health: Companies would later publish much of this work in health promotion materials for their own clients, thus spreading the medical model of precise measurement into the domestic sphere. Overweight is a burden, not a reserve fund. Thus, by the end of the nineteenth century, the ideal of a quantified norm of healthy weight at least for infants and children was well established, both in professional circles and in many middle-class homes. However, its move into general medical practice and out of the domestic nursery would be more gradual and less comprehensive. Indeed some doctors expressed specific resistance to standardised classificationism of adults, which they claimed bore little relevance to individuals, including overweight individuals. Although no very great size or weight, still I could not stoop to tie my shoe, so to speak, nor attend to the little offices humanity requires without considerable pain and difficulty, which only the corpulent can understand; I have been compelled to go down stairs slowly backwards, to save the jar of increased weight upon the ankle [sic] and knee joint, and been obliged to puff and blow with every slight exertion. He detached dietary interventions from medical therapy and placed them firmly in the realm of self-help and self-monitoring. Fat, or, Embonpoint, in Excess. The plan of treatment is simple, and in its explanation devoid of all medical mystification. A Treatise on Corpulency, first published in , urged that being overweight required the intervention of a physician, who would provide treatment, an individual diet plan, and crucially the necessary moral support to carry out a cure. While claiming to draw on scientific knowledge and approaches to fix the problem, and emphasising careful regulation by the physician, his diet plan relied largely on the straightforward correction of the diet and additional exercise. Yorke-Davies provided his readers with recipes and advice on food intake based on hospital dietaries and in relation to expenditure of effort in work and physical activity. Food was to be carefully weighed, and reports of successful weight loss indicated that his

dieters, too, were regularly weighed recording their week-by-week weight reduction. His most famous diet patient was American President William Howard Taft , who hired York-Davies to supervise his weight loss programme. The two corresponded regularly for over 20 years and Taft kept a daily record of his weight, alongside details of his food intake and physical activity. In fact, the acquisition of accurate and comprehensive measurements of height and weight for healthy adults proved a greater challenge than was the case for infants. Initially demanding complex systems of weights and the specific positioning of individuals under surveillance, early instruments for quantifying adult body weight made them unlikely domestic or indeed clinical technologies. Moreover, as the editors of the Lancet indicated in , personal weighing scales had been too large and too expensive even for use in medical consulting rooms, much less domestic spaces, though new designs promised cheaper and more compact solutions. Users required training expertise and often a second pair of hands to produce accurate measurements. They would likewise be taught to measure themselves and their children against standardised height and weight curves. In his diet book, A. One of the chief institutions of Carlsbad is the weighing machine; nowhere do you see so many weighing machines. Many were clearly weighing themselves regularly and checking for weight loss and weight maintenance. Other clients, however, reported that it was not convenient to get weighed, and defined their success by other means, both quantifiable and experiential. My appearance and feelings tell me I am sufficiently reduced; but what I am most thankful for is feeling so much better. I have quite lost that dreadful feeling of oppression and weight. And as Katherine Vester has demonstrated for American consumers, this is exactly what they did. As we have seen, however, popular cultures of self-surveillance got a head-start from the emergence of the penny-scales as a form of entertainment and self-help. For adults, at least, self-measurement was often a public activity, appealing to both men and women. Fortescue Flannery, chairman of W. Avery, Ltd one of two major UK manufacturers of weighing equipment proudly informed his shareholders at the Annual Meeting: Selling Health through the Bathroom Scale As ideals of precision and quantification entered public, domestic and professional understandings of health, what became of the home as a site of health care, consumption and decision making in the twentieth century? For decades, historians of medicine have told a story about the rise of science and the rise of the medical profession. Closer attention to practices within the household, however, may challenge this implied correspondence between the growing cultural capital of biomedicine, and increases in its reach and impact on the ground or in the home. Drawing on the example of the bathroom scale in Britain, the remainder of this paper will explore the twentieth-century rise of quantitative, technologised self-surveillance as a domestic, home-based culture of health promotion, and an established health-seeking behaviour. Even after the invention of the relatively small spring-balance platform scale in the s, the purchase of a domestic adult scale represented a significant investment in self-surveillance even for a middle-class household. These scales appeared alongside an array of precision measuring equipment, from dispensing scales to graduated infant feeding bottles.

Chapter 4 : Bulletin June/July

For the last few months, I've been tracking my activities, location, happiness, sleep cycles, among other things, using fun tech gadgets (such as the Fitbit) and smartphone apps. I had to trade my.

Peter Maass November 13 , 9: Their project, somewhere between art and porn, hovers on the R-rated margins of a thriving cultural movement in which artists of all stripes are exploring what it means to live in a state of surveillance. They are the opposite of the acronym-laden news stories we read: They are playful, invasive and eerie, and best of all they are graphically visual. With a transgressive edge that journalism struggles to match, they creatively challenge what it means to be human in a time of data. The stunner in this show is an object created by Hasan Elahi that from a distance looks like a lovely tapestry draped on a wall. As Elahi has explained , in he was stopped at the Detroit airport because his name appeared on a terrorism watchlist, and he was subsequently interrogated by FBI agents. Born in Bangladesh and raised in the United States, Elahi, an art professor at the University of Maryland, chose an unusual response to clear his name and make a statementâ€”he began a self-surveillance project in which he took pictures of nearly everything he did and sent them to the FBI. He also posted them to a website he created. It works on several levels. Aesthetically and from afar, it is a gorgeous, softly-colored flag, something Jasper Johns might have created with fabric. His artwork is the analog turned digital turned material. Walker Evans led the way with undercover pictures taken on the New York City subway with a Leica hidden behind his coat. The wave seems to have grown larger in the wake of the leaks from NSA whistleblower Edward Snowden, and this is fortunate. We need to see it anew. The project engages you far more deeply than a stack of original documents or news stories about them ever could. The exhibit offers much moreâ€”photojournalist Tomas van Houtryve displays his beautiful and disturbing pictures taken with a small drone that he flew over American settings to replicate the locations of drone strikes in Pakistan and Afghanistanâ€”weddings, playgrounds, people praying or exercising. There is also the turn-the-tables work of Simon Menner, a German who combed through the Stasi archives for pictures the East German spy agency took of its own agents mainly in training situations, but also at parties. The effect is literally destabilizingâ€”with the code names rising as you stand still, you feel as though you are falling in a shaft of infinite surveillance. Paglen materializes our political vertigo. For instance, artist Heather Dewey-Hagborg has collected DNA samples from cigarette butts, chewing gum and stray hair, and has used these to create portraits of whomever the DNA belongs to.

Chapter 5 : Gary T. Marx - Encyclopedia of Social Theory: Surveillance

Like lots of people, I'm paying attention to the Apple Watch buzz, and doing some of my own speculation. Needless to say, I have no special expertise here. But what the heck; I might as well put my own thoughts out there. So, here's my pathetic version of a grand insight: wearables like the.

Click search or press enter Self Surveillance by Kate Greene September 10, The simple pedometer has been given a makeover. Data is wirelessly uploaded to the Web so that users can monitor their activity and compare it with that of their friends. Every step you take: James Park , cofounder of Fitbit, says that one of the main goals was to make the sensor so small that it will go unnoticed no matter what a person is wearing. The device can be put in a pocket, attached discreetly to a bra, or slipped into a special wristband during sleep. It is meant to be worn , and each device can run for 10 days on a single battery charge. Park demonstrated the Fitbit device in San Francisco on Tuesday at the Techcrunch50 conference, a popular launch pad for new technology companies. He says that Fitbit is tapping into an important field of wearable sensors and personal health monitoring: For years, runners and walkers have used pedometers to track their exercise routines, but these devices can be relatively bulky and provide only a limited amount of information. Some newer pedometers connect to computers so that people can track their exercising in detail, but the process is often cumbersome. The shoes transmit data to an iPod that, in turn, uploads the data to the Web when the iPod is synced with a computer. During his demonstration at the conference, Park walked onstage for 17 steps, past the Fitbit base station. He then refreshed his information on the Fitbit website to show that his total steps for the day had already been updated. Importantly, Park noted that Fitbit has built-in technology to distinguish between the motion of a car and a person walking or running. Data from the Fitbit sensor is automatically uploaded to the internet via a base station. A person accesses her Fitbit data through a personalized page that highlights physical activity, calories burned, and sleep patterns. She can also create a social network of friends, family members, or co-workers who want to share activity data. Another feature that Park believes sets Fitbit apart is the way that its Web service automatically converts steps taken into burned calories and lets people compare their activity with that of other Fitbit users. The site can also log meals and create calorie budgets to tie into a diet regime. At night, the sensor fits into a wristband, and its accelerometer tracks tiny tremors in the wrist that correlate to different stages of sleep. When sleep-related data is uploaded to the Web, it is used to create a graph showing the amount and quality of sleep achieved each night.

Chapter 6 : Surveillance - Wikipedia

It's just a microcosm of today's vibrant surveillance art scene. Travel a few dozen blocks from the Open Society and you'll reach the latest work by Trevor Paglen, who has collected more.

Marx This article offers a broad overview and introduction. Traditional Surveillance An organized crime figure is sentenced to prison based on telephone wiretaps. A member of a protest group is discovered to be a police informer. To varying degrees it is a property of any social system --from two friends to a workplace to government. Each of these also involves surveillance. Information boundaries and contests are found in all societies and beyond that in all living systems. Humans are curious and also seek to protect their informational borders. To survive, individuals and groups engage in, and guard against, surveillance. However the form, content and rules of surveillance vary considerably --from relying on informers, to intercepting smoke signals, to taking satellite photographs. In the 15th century religious surveillance was a powerful and dominant form. This involved the search for heretics, devils and witches, as well as the more routine policing of religious consciousness, rituals and rules e. Religious organizations also kept basic records of births, marriages, baptisms and deaths. In the 16th century, with the appearance and growth of the embryonic nation-state, which had both new needs and a developing capacity to gather and use information, political surveillance became increasingly important relative to religious surveillance. Forms such as an expanded census, police and other registries, identity documents and inspections appeared which blurred the line between direct political surveillance and a neutral even in some ways more benign, governance or administration. Such forms were used for taxation, conscription, law enforcement, border control both immigration and emigration , and later to determine citizenship, eligibility for democratic participation and in social planning. In the 19th and 20th centuries with the growth of the factory system, national and international economies, bureaucracy and the regulated and welfare states, the content of surveillance expanded yet again to the collection of detailed personal information in order to enhance productivity and commerce, to protect public health, to determine conformity with an ever-increasing number of laws and regulations and to determine eligibility for various welfare and intervention programs such as Social Security and the protection of children. Government uses in turn have been supplemented and on any quantitative scale likely overtaken by contemporary private sector uses of surveillance at work, in the market place and in medical, banking and insurance settings. A credentialed state, bureaucratically organized around the certification of identity, experience and competence is dependent on the collection of personal information. Reliance on surveillance technologies for authenticating identity has increased as remote non face-to-face interactions across distances and interactions with strangers have increased. Modern urban society contrasts markedly with the small town or rural community where face-to-face interaction with those personally known was more common. The microchip and computer are of course central to surveillance developments and in turn reflect broader social forces set in motion with industrialization. The increased availability of personal information is a tiny strand in the constant expansion in knowledge witnessed in the last two centuries, and of the centrality of information to the workings of contemporary society. The New Surveillance The traditional forms of surveillance noted in the opening paragraph contrast in important ways with what can be called the new surveillance, a form that became increasingly prominent toward the end of the 20th century. The new social surveillance can be defined as, "scrutiny through the use of technical means to extract or create personal or group data, whether from individuals or contexts". The use of "technical means" to extract and create the information implies the ability to go beyond what is offered to the unaided senses or voluntarily reported. Much new surveillance involves an automated process and extends the senses and cognitive abilities through using material artifacts or software. Yet the eye as the major means of direct surveillance is increasingly joined or replaced by other means. The use of multiple senses and sources of data is an important characteristic of much of the new surveillance. Traditionally surveillance involved close observation by a person not a machine. But with contemporary practices surveillance may be carried out from afar, as with satellite images or the remote monitoring of communications and work. Nor need it be close as in detailed, --much initial surveillance involves superficial

scans looking for patterns of interest to be pursued later in greater detail. Surveillance has become both farther away and closer than previously. It occurs with sponge-like absorbency and laser-like specificity. In a striking innovation, surveillance is also applied to contexts geographical places and spaces, particular time periods, networks, systems and categories of person, not just to a particular person whose identity is known beforehand. The new surveillance technologies are often applied categorically. Traditional surveillance often implied a non-cooperative relationship and a clear distinction between the object of surveillance and the person carrying it out. In an age of servants listening behind closed doors, binoculars and telegraph interceptions that separation made sense. It was easy to distinguish the watcher from the person watched. Yet for the new surveillance with its expanded forms of self-surveillance and cooperative surveillance, the easy distinction between agent and subject of surveillance can be blurred. Bentham proposed a highly organized system for managing large populations within physically enclosed structures such as a prison, a factory or a school, in which authorities could see all, but not be seen. From a standpoint of social control this created uncertainty. Inmates could never be sure when they were being watched and hence through self-interest and habit it was hoped they would engage in self-discipline. Well-publicized contemporary warnings. A general ethos of self-surveillance is also encouraged by the availability of products that permit individuals to test themselves. Implanted chips transmitting identity and location which were initially offered for pets, are now available for their owners and others as well. In some work setting smart badges worn by individuals do the same thing, although not with the same degree of voluntarism. The new surveillance relative to traditional surveillance has low visibility, or is invisible. Manipulation as against direct coercion has become more prominent. Monitoring may be purposefully disguised as with a video camera hidden in a teddy bear or a clock. Or it may simply come to be routinized and taken for granted as data collection is integrated into everyday activities. The relatively labor-intensive bar code on consumer goods which requires manually scanning may soon be replaced with inexpensive embedded RFID Radio Frequency Identification computer chips which can be automatically read from short distances. The remote sensing of preferences and behavior offers many advantages such as controlling temperature and lighting in a room or reducing shipping and merchandising costs, while also generating records that can be used for surveillance. There may be only a short interval between the discovery of the information and the automatic taking of action. The individual as a subject of data collection and analysis may also almost simultaneously become the object of an intervention, whether this involves the triggering of an alarm or the granting or denial of some form of access. The new forms are relatively inexpensive per unit of data collected. Relative to traditional forms it is easy to combine visual, auditory, text and numerical data. It is relatively easier to organize, store, retrieve, analyze, send and receive data. Data are available in real time and data collection can be continuous and offer information on the past, present and future ala statistical predictions. Simulated models of behavior are created. The new surveillance is more comprehensive, intensive and extensive. The ratio of what the individual knows about him or herself relative to what the surveilling organization knows is lower than in the past, even if objectively much more is known. One way to think about the topic is to note that many of the kinds of surveillance once found only in high security military and prison settings are seeping into the society at large. Are we moving toward becoming a maximum security society where ever more of our behavior is known and subject to control? Six features of the maximum security society are 1 a dossier society in which computerized records play a major role 2 an actuarial society in which decisions are increasingly made on the basis of predictions about future behavior as a result of membership in, and comparisons to, aggregate categories 3 a suspicious society in which every one is suspected 4 an engineered society in which choices are increasingly limited and determined by the physical and social environment 5 a transparent society, in which the boundaries of time, distance, darkness, and physical barriers that traditionally protected information are weakened and 6 a self-monitored society, in which auto-surveillance plays a prominent role. Surveillance Structures Several kinds of social structure define surveillance relationships. There is an important difference between organizational surveillance and the non-organizational surveillance carried about by individuals. Large organizations have become ever more important in affecting the life chances of individuals. Organizations are the driving force in the instrumental collection of personal data. At the organizational level formal surveillance

involves a constituency. Constituency is used broadly to refer to those with some rule-defined relationship or potential connection to the organization, whether this involves formal membership, or merely forms of interaction with it such as renting a video or showing a passport at a border. All organizations have varying degrees of internal and external surveillance. They belong as members. There is often a loose analogy to the ownership of property. External constituency surveillance involves watching those who have some patterned contact with the organization, e. Credit card companies and banks for example monitor client transactions and also seek potential clients by mining and combining data bases. Or consider the control activities of a government agency charged with enforcing health and safety regulations. Such an organization is responsible for seeing that categories of person subject to its rules are in compliance, even though they are not members of the organization. Non-governmental organizations that audit, grant ratings, licenses and certifications have the same compliance function. Organizations also engage in external non-constituency surveillance in monitoring their broader environment in watching other organizations and social trends. The rapidly growing field of business intelligence seeks information about competitors, social conditions and trends that may effect an organization. Industrial espionage is one variant. Planning also requires such data, although it is usually treated in the aggregate rather than in personally identifiable form. With the widespread accessibility democratization? This may involve role relationship surveillance as with family members parents and children, the suspicious spouse or friends looking out for each other e. Or it can involve non-role relationship surveillance, as with the free-floating activities of the voyeur whose watching is unconnected to a legitimate role. All persons play both roles, although hardly in the same form or degree, and this shifts depending on the context and over the life cycle and as noted the roles are sometimes blurred. Within the surveillance agent category the surveillance function may be central to the role, as with police, private detectives, spies, work supervisors and investigative reporters. Or it may simply be a peripheral part of a broader role whose main goals are elsewhere, as with check-out clerks who are trained to look for shop lifters, or dentists who are encouraged or required to report suspected child abuse when seeing bruises on the face. A distinction rich with empirical and ethical implications is whether the situation involves those who are a party to the generation and collection of data direct participants or instead involves a third party. A third party may legitimately obtain personal information through contracting with the surveillance agent e. Or it may be obtained because confidentiality is violated by the agent, or because an outsider illegitimately obtains it wiretaps, hacking. An important distinction that often involves power differentials is whether the surveillance is non-reciprocal or reciprocal. The former is one-way with personal data going from the watched to the watcher e. With reciprocal surveillance it is bi-directional e. Surveillance that is reciprocal may be asymmetrical or symmetrical with respect to means and goals. Thus in a democratic society citizens and government engage in reciprocal but distinct forms of mutual surveillance. For example citizens can watch government through Freedom of Information Requests, open hearings and meetings, and conflict of interest and other disclosures required as a condition for running for office. In bounded settings such as a protest demonstration, there may be greater equivalence with respect to particular means e. In organizational settings, power is rarely all on one side, whatever the contours of formal authority.

Chapter 7 : self-surveillance - definition and meaning

Governmentality is a conceptualization of power that accounts for the role of disciplining institutions in mass-population surveillance and social control.

See other articles in PMC that cite the published article. Introduction When asked how they view doping within their sport, many non-elite runners immediately begin discussing the activities of elite or professional runners. Elite athletes are subject to constant surveillance through increased testing protocols and programs such as the athlete biological passport ABP program, they are forced to comply with doping regulations set out by the World Anti-Doping Agency WADA in order to compete, and the names of elite runners continually show up in newspapers when doping scandals occur. Yet, the effects of these anti-doping efforts do not simply stop at the line between elite and non-elite runners. They also bleed into the everyday practices of the non-elite runner. Anti-doping surveillance technologies are directed at the high-risk population Dean of elite athletes. Elite runners are regarded as suspicious in terms of doping and PED use because the perceived stakes of winning a competitionâ€”prize money, often in large amounts; sponsorship deals resulting from major winsâ€”are high enough that elites may be tempted to use PEDs. Elite surveillance works to discipline runners by monitoring their bodies in order to detect the presence of banned substances or doping methods. Because they can be tested at anytime, elites must conform to anti-doping regulations or face sanctions, including bans from competition WADA Non-elite runners, in contrast, generally do not rely on race winnings as a primary source of income. As the stakes are perceived to be much lower, so too are the risks of doping, which do not warrant direct biological surveillance. This paper explores disciplining effects of current anti-doping surveillance systems on the daily behaviors, habits and health consequences of non-elite runners. As this group is not exposed to direct anti-doping testing and enforcement, it is tempting to argue non-elites are unaffected by anti-doping efforts that target the elite level of their sport. However, because non-elite runners are not subject to anti-doping surveillance systems nor are forced to comply with anti-doping regulations, they are implicated within the wider arena of disciplinary power that envelops both elite and non-elite athletes and anti-doping agencies. Non-elite runners report engaging in self-surveillance in their training and supplementing practices, often relying on those they view as experts when making decisions about how to enhance their performances with minimal risk to their health and to ensure conformity to the rules and norms of their sport as far as they understand them. Since their knowledge of banned substances is largely derived from media accounts of elites who are caught doping, many non-elite runners have only a superficial and sometimes incorrect understanding of doping. Many view doping and its associated health risks as a problem only of elite running that remains limited to only a handful of widely publicized PEDs or doping methods. These arguments are followed by a brief description on doping in the sport of running and of the rise of the current anti-doping approaches. This paper argues the current elite surveillance-based systems of anti-doping can work against the health promotion goals of anti-doping agencies by leading non-elites to self-surveil only to the extent that they are following the rules as they understand them. This process leads to a blind spot in the internalized anti-doping gaze that allows non-elite runners to simultaneously engage in self-surveillance while taking for granted the safety and perceived benefits of unregulated and non-banned nutritional supplements. I examine various ways these mis understandings inform how non-elite runners engage in self-surveillance to ensure they remain within the normative bounds of their sport when making decisions as to which products to use in their own training. Surveillance and Sport One way to view anti-doping efforts is as a result of external control exercised on athletes by forcing them to yield to a repressive form of surveillance and power. Foucault described the role of disciplining institutions, including schools, prisons, and the military, in exposing individuals to normalizing rules, authorities, and habits. Through such processes of normalization, disciplinary power does not necessarily repress but invests disciplined bodies with strongly internalized norms Rail and Harvey Within the sporting context, athletic bodies are subject to the one-way gaze of anti-doping agencies through the Panoptic metaphor. Governmentality is a conceptualization of power that accounts for the role of disciplining institutions in mass-population surveillance and social control. Instead of seeing power as

exclusively state held and top-down Foucault , the governmentality ensemble is aimed at shaping individuals to autonomously care for and govern themselves and each other based on internalized knowledges and discourses that inform and direct their behavior. Foucault explained that governmentality was: This form of governance includes disseminating expert knowledge on how to properly behave and make decisions in the development and care of oneself Rose Working through apparatuses such as schools, hospitals, or sports, disciplinary techniques aid in the administration of the social body by producing knowledge of the population through statistics reflecting medical, criminal, and institutional expertise. Instead of bureaucracies directing modes to promote individual health, experts offer instruction and advice based on the assumption that individuals want to be healthy Rose , 86â€” Rose argues experts, such as sports officials and medical professionals, offer advice and guidance to populations in effort to direct their decisions towards institutionally established goals of promoting health for the entire population. Anti-doping experts have used such health promotion philosophies as a foundational justification for their efforts to target elite athletes since the s. Linking sport participation with healthy lifestyles, labeling banned substances as contrary to good health, and attaching social shame to poor health choices, work together to make bans on certain substances appear logical and in promoting self-discipline amongst athletes. Health and the best ways of achieving it are presented to the individual as both a choice and a broader social obligation Rose , Equally, doping is considered a matter of individual choice that can lead to competition bans when athletes are tested and detected. However, for non-elites who are not subject to testing, the threats of negative health outcomes from doping appear contribute to different forms of self-surveillance. Through these processes external forms of mass-population surveillance and regulation give way to self-surveillance. Doping and Running Despite the long history of performance enhancing substances in various sports Mazanov and McDermott , it is only since the s following the televised death of a Tour de France cyclist who was engaging in doping, that doping has been identified as a problem for both sports and athletes Waddington Since then, track and road runners have been at the center of doping scandals as much as athletes in other sports. This list is updated annually to prohibit those products and procedures that are considered to be illicit doping agents or practices WADA Banned substances include items such as anabolic steroids, as well as some less familiar products such as diuretics. The federated system of anti-doping bureaucracies provides multiple levels of testing surveillanceâ€”from the local race organizer to international bodies at World Championship eventsâ€”and conducts extensive surveillance focusing mainly on elite athletes. The ABP expands on some of the previous limitations of illicit drug testing by allowing agencies to compile a biological profile for each athlete that can track changes in blood markers that are suggestive of doping WADA APB These biological surveillance systems are intended to deter athletes from using prohibited and potentially harmful substances by decreasing their ability to mask or cycle their consumption, while allowing testers to track changes in particular blood makers indicative of some form of doping. Despite this increasing surveillance, the pervasiveness of doping at the elite level remains unknown. Those with the closest proximity to road athletes attest that doping is indeed a problem within the sport. Though non-elite runners are subject to the same rules as elites, they are not targeted for doping tests. One reason often cited for the lack of testing at the elite level is the prohibitive costs Monti One can reasonably presume the same argument applies to the testing of non-elite runners, especially if they are assumed to have little monetary or commercial incentive to resort to doping. Difficulty determining the prevalence of doping at the non-elite level is compounded by their lack of understanding of doping rules and prohibited substances Laure Several studies on athletes and supplementation have suggested many elite and non-elite athletes use dietary supplements with the belief they may enhance performance Baume, Hellemans, Saugy Suzic Lazic et al. Though dietary supplements are not banned, often due to mislabeling and problems of cross-contamination during manufacturing, they cannot be assumed free of banned substances, as they are not regulated by any agency in the way food or medications are regulated by organizations such as the Food and Drug Administration FDA. While supplement manufacturers are required to report adverse health outcomes related to supplements to the FDA, and as many as 50, adverse events are estimated to occur annually, relatively few are formally reported Cohen Anti-doping agencies have also issued warnings to athletes to beware of certain supplements and USADA has a page on its website [http:](http://) Troublingly, Harel et al

found that supplement recalls are not necessarily mandated or carried out even when the FDA confirms the existence of contamination. The recent death of a non-elite marathon runner linked to use of the unregulated energy supplement DMAA contained in product Jack3d demonstrates that such products are readily used by athletes who may not be fully aware of the associated risks to their health Hamilton The widespread use and availability of supplements normalizes their presence in the training regimens of non-elite runners. These processes of normalization mean that over time athletes who engage with the risk on a day-to-day basis consider the overall health risks to be mundane Albert Maughan, Greenhaff, and Hespel caution that as athletes become more and more desensitized to taking and using supplements, they will initially exercise caution in order to minimize health risks from novel supplements that lack in institutional research on their efficacy and safety, which erodes gradually over time as their use of these supplements becomes routine.

Surveillance and Discipline of Runners The bodies of runners are on display when they compete in races. As anti-doping efforts rely increasingly on biological surveillance systems, intimately personal markers of doping that were previously invisible are rendered visible. For elite athletes, testing has led to a shift from surveilling what is visible on the body to surveillance of what is made visible from within the body. These values simultaneously pathologize any athlete who departs from this standard through doping or use of PEDs. The inner self of the athlete is also implicated in biological test results. Deleuze posited that what we can say about bodies depends to a large extent on what we can see, and what we can see is bound up in the underlying discourses that actively produce and establish the truth of the subjects for which they speak. Thus, biological anti-doping regimes produce the truth of what constitutes athletes as a group, as well as the acceptable behaviors and ways of being an individual athlete. No longer reliant on the exterior visual field of athletic bodies, biological testing allows the truth of the inner self of the athlete to be read from formerly invisible matter through a microscope Deleuze Body and self become indistinguishable, then are categorized as normal in the case of a negative test, or pathological if banned substances are found. For runners, negative tests indicate a morally good, clean inner-self, while positive tests signify the flawed and dirty, morally corrupt character. Biological testing expands what is visible, and therefore readable, only for those who undergo the test. The biology of non-elite runners, and hence their own inner truth, remains hidden, unseen and unread. Nevertheless, through observing the self and others Rail and Harvey the pervasive anti-doping gaze in contemporary elite sport promotes various forms of self-surveillance amongst non-elite athletes. Internalizing this gaze leads runners to self-surveil to ensure their conformity to the clean ideal by following the dictates of the running environment Shogan even when they are not exposed to or remain outside these formal biological surveillance processes Lang When there are differences in what is understood as normal, healthy or acceptable between rule-makers such as WADA and individual, the result is a potential blind spot in the internalized gaze. For non-elite runners many of the lesser known banned substances and potentially harmful but legal substances are located in this blind spot. As their internalized gaze is not as clear as that of the elite runner, non-elite runners may mistakenly make decisions they view as correct or healthy but that may result in short-, long-term or even fatal consequences.

Methods The runners interviewed for this work were part of a larger project on non-elite runners and doping. Interviews were conducted using a semi-structured interview format with non-elite runners based in New York City. The reasoning behind limiting this sample to NYRR-affiliated team members is three-fold. First, team affiliation requires some form of interaction with other runners, as opposed to fitness, recreational, or competitive solo runners who tend to work out alone or do not interact with others. Second, as many runners may not race to win or place, the team competition structure provides a team-oriented goal that can induce runners to race regularly in order to field a points-scoring team, while providing a competitive goal outside of their own personal motivations. Third, individuals competing in NYRR-sponsored races are required to agree to the rules of competition when registering for a race, including conforming to anti-doping regulations. Therefore, racing for an affiliated team ensures that runners have agreed to a formal anti-doping code of conduct. Recruitment of interview participants began from my own position as a non-elite runner and built outward through the networks of initial interviewees. The sample is a result four waves of recruitment. As a condition of taking part in this study, each interviewee provided contact information for any three non-elite runners fitting the study criteria, who were then notified of the

recommendation from another runner who had taken part in the study. This networking method, while similar to a snowball sampling method, has many advantages for qualitative research. Recruitment drew participants from up to five degrees of separation from myself. This distance ensured that participants differ from those derived solely from the personal network of the author, providing a sufficient sample that does not contain biases often found in snowball samples Semaan, Lauby, and Liebman Twenty-eight semi-structured interviews were conducted between June and April This semi-structured interviewing method allowed for flexibility during the discussion Schensul et al. The audio-recorded interviews were transcribed and the data organized using the qualitative analysis software Atlas. Coding was guided by the three main thematic categories established in the interview guideâ€”knowledge, ethics, and healthâ€”while several second-order categories were drawn from directly from the data that covered specific topics emerging during the interviews e. Non-Elite Self-Surveillance The non-elite runners interviewed for this project routinely engage in self-surveillance for the sake of both performance and health. They keep logs of how much mileage they run daily, weekly, and monthly, record mile split times on training runs, are vigilant about how they recover from hard workouts and racing efforts, and keep track of their diet in order to maintain a specific weight and to ensure they eat the correct balance of carbohydrates, fats, and proteins. These runners also report experimenting with and regularly using nutritional supplements as part of their surveillance process. The runners describe these processes as conscious and on-going routines.

Chapter 8 : Self-surveillance: Should you worry or simply embrace your personal data?

norms through self-surveillance and self-disciplinary practices, especially those of the body such as the self-regulation of hygiene, health, and sexuality.

The vast majority of computer surveillance involves the monitoring of data and traffic on the Internet. A Packet Capture Appliance intercepts these packets, so that they may be examined and analyzed. Thus, automated Internet surveillance computers sift through the vast amount of intercepted Internet traffic, filtering out, and reporting to investigators those bits of information which are "interesting", for example, the use of certain words or phrases, visiting certain types of web sites, or communicating via email or chat with a certain individual or group. More people are potentially subject to Internet surveillance. There are advantages and disadvantages to network monitoring. For instance, systems described as "Web 2.0". One researcher from Uppsala University said "Web 2.0". We can characterize Web 2.0. Yet, employers themselves also monitor their employees. A research group states "The virtual assistant has become a social integration into lives. If the law enforcement are able to be called using a virtual assistant, the law enforcement would then be able to have access to all the information saved for the device. The devices are listening to every conversation the owner is having. Even if the owner is not talking to a virtual assistant, the device is still listening to the conversation in hopes that the owner will need assistance, as well as to gather data. Computer surveillance in the workplace Corporate surveillance of computer activity is very common. The data collected is most often used for marketing purposes or sold to other corporations, but is also regularly shared with government agencies. The data can be also sold to other corporations so that they can use it for the aforementioned purpose, or it can be used for direct marketing purposes, such as targeted advertisements, where ads are targeted to the user of the search engine by analyzing their search history and emails [23] if they use free webmail services, which are kept in a database. Preventing misuse of resources. Companies can discourage unproductive personal activities such as online shopping or web surfing on company time. Monitoring employee performance is one way to reduce unnecessary network traffic and reduce the consumption of network bandwidth. Promoting adherence to policies. Online surveillance is one means of verifying employee observance of company networking policies. Firms can be held liable for discrimination or employee harassment in the workplace. Organizations can also be involved in infringement suits through employees that distribute copyrighted material over corporate networks. Federal legislation requires organizations to protect personal information. Monitoring can determine the extent of compliance with company policies and programs overseeing information security. Monitoring may also deter unlawful appropriation of personal information, and potential spam or viruses. The protection of intellectual property, trade secrets, and business strategies is a major concern. The ease of information transmission and storage makes it imperative to monitor employee actions as part of a broader policy. A second component of prevention is determining the ownership of technology resources. For instance, Google search stores identifying information for each web search. An IP address and the search phrase used are stored in a database for up to 18 months. This information, along with the information from their email accounts, and search engine histories, is stored by Google to use to build a profile of the user to deliver better-targeted advertising. The Department of Homeland Security has openly stated that it uses data collected from consumer credit and direct marketing agencies for augmenting the profiles of individuals that it is monitoring. Normal keylogging programs store their data on the local hard drive, but some are programmed to automatically transmit data over the network to a remote computer or Web server. There are multiple ways of installing such software. The most common is remote installation, using a backdoor created by a computer virus or trojan. This tactic has the advantage of potentially subjecting multiple computers to surveillance. Viruses often spread to thousands or millions of computers, and leave "backdoors" which are accessible over a network connection, and enable an intruder to remotely install software and execute commands. More often, however, viruses created by other people or spyware installed by marketing agencies can be used to gain access through the security breaches that they create. An attacker can then install surveillance software remotely. Servers and computers with permanent broadband connections are most vulnerable to this type of

attack. This method shares a disadvantage with hardware devices in that it requires physical access to the computer. These social network "maps" are then data mined to extract useful information such as personal interests, friendships and affiliations, wants, beliefs, thoughts, and activities. These types of threats are most easily countered by finding important nodes in the network, and removing them. To do this requires a detailed map of the network. The purpose of the SSNA algorithms program is to extend techniques of social network analysis to assist with distinguishing potential terrorist cells from legitimate groups of people. In order to be successful SSNA will require information on the social interactions of the majority of people around the globe. Since the Defense Department cannot easily distinguish between peaceful citizens and terrorists, it will be necessary for them to gather data on innocent civilians as well as on potential terrorists. This form of computer surveillance, known as TEMPEST, involves reading electromagnetic emanations from computing devices in order to extract data from them at distances of hundreds of meters. The Clipper Chip, formerly known as MYK, is a small hardware chip that the government can install into phones, designed in the nineties. It is intended to secure private communication and data by reading voice messages that are encoded and decode them. This has led to the failure of the Clipper proposal, even though there have been many attempts. Had CBDTPA become law, it would have prohibited technology that could be used to read digital content under copyright such as music, video, and e-books without Digital Rights Management DRM that prevented access to this material without the permission of the copyright holder. Surveillance as an aid to censorship[edit] See also: Internet censorship and Internet censorship circumvention Surveillance and censorship are different. Surveillance can be performed without censorship, but it is harder to engage in censorship without some form of surveillance. The report includes a list of "State Enemies of the Internet", Bahrain, China, Iran, Syria, and Vietnam, countries whose governments are involved in active, intrusive surveillance of news providers, resulting in grave violations of freedom of information and human rights. Computer and network surveillance is on the increase in these countries. Neither list is exhaustive and they are likely to be expanded in the future. Journalists should equip themselves with a "digital survival kit" if they are exchanging sensitive information online, storing it on a computer hard-drive or mobile phone.

Chapter 9 : Self Surveillance - MIT Technology Review

As we have seen, however, popular cultures of self-surveillance got a head-start from the emergence of the penny-scales as a form of entertainment and self-help. For adults, at least, self-measurement was often a public activity, appealing to both men and women.