DOI: 10.1145/1743546.1743582

BY JAN KIETZMANN AND IAN ANGELL

# Panopticon Revisited

THE YEAR IS 1787. UTILITARIAN PHILOSOPHER Jeremy Bentham publishes his ideas for a panopticon, a quite brilliant merger of architectural design with an understanding of human behavior. This is a prison requiring minimal supervision. It is circular in cross-section. Cells are placed on the circumference, stacked floor upon floor, with the doors facing a guard tower at the centre. That tower is designed so that a lone guard can see every point of the prison from behind a mesh screen – he can see the prisoners, each uniquely identified, but they can't see him. Not knowing if they are being watched, but having to assume that they are, the prisoners adjust their behavior. At regular intervals, each prisoner is relocated according to his overall record of discipline – good behavior is rewarded, bad conduct punished. Ergo, a highly efficient and cost effective method for controlling sociopaths, and thereby regulating the prison.

Fast-forward to the first decade of the 21 century, and Closed Circuit Television (CCTV). The panopticon is no longer just a concept for prisons. Manhattan's Chinatown has seen an increase from 13 to 600 'security' cameras since 1998.4 Britain alone has 20% of the world's CCTV cameras, which watch traffic, shoppers, and people walking down the street, all on the lookout for sociopathic acts. British subjects going about their ordinary lives can expect to be captured on camera 300 times a day, every day. George Orwell would have been proud and horrified to see that his vision of a society monitored by cameras and computers is quickly becoming a reality; and he wouldn't be amazed that the most recent generation of cameras can also reprimand offenders in a child's voice broadcast over loudspeakers.[3]

These location-specific technologies, embedded into the fabric of social life, allow uniformed officials who gaze at screens to 'monitor' and judge whether or not acts are antisocial. But of course such evidence can at best help identify suspects after the event, as was the case in London's 2005 bombing, and the abduction and murder in 1993 of two-year old Jamie Bulger in Liverpool. A recent report into the London's surveillance network claimed that only one crime is solved by each 1,000 CCTV cameras.[2] More importantly, the technology does not stop these acts *in flagrante delicto*. Bad-deeds still happen. To be consistent with the panopticon concept, the state therefore still needs to instill the belief in the population that the very presence of monitoring artifacts means the virtual attendance of authority: that being caught red-handed on camera undoubtedly leads to punishment and perhaps prison sentences. The ability to watch antisocial behavior, and the presence of such dedicated technologies, should therefore positively direct social behavior.

The problem is that using surveillance technology involves both equipping every dark corner with a CCTV camera, and manning a remote monitor with a 'warm body' city official who will watch the happenings from afar. CCTV is not a cost-sensitive approach, and as David Davis MP, the former U.K. Shadow Home Secretary comments, it "leads to massive expense and minimum effectiveness."[10] As a result, authorities have privatized some of these duties: private parking attendants assign tickets; and citizens armed with city-licensed radar guns hunt speeders for extra income (and excitement) during retirement.[8]

Of course, the outsourcing of such government services is still a far cry from a panopticon; it is solely exercising policing but in a different form.

Nevertheless, to a certain extent the authorities have already turned to the cost-effective lessons of the panopticon. Accordingly, fake CCTV cameras and mock-ups of speed traps are set up, and even cardboard billboards of police cruisers are mounted to the rails of bridges over highways, in the hope of creating a similar reaction to seeing real cameras, traps and cars. However, in the resulting 'climate of suspicion,' such replicas can lead, paradoxically, to increased accident rates, and even higher speeds once drivers spot the dummies. 'Criminals' are quick to identify real cameras from the fake, or they simply displace their 'business' to locations that lack obvious threats. Clearly, such attempts can create more problems than they solve.

However, that was only the first generation panopticon, which in order to direct social behavior, represented a reactive approach by authority to disobedience, and focused on punishment, or the threat there of. Little effort was aimed at either understanding the reasons for such behavior, or managing the motivation of social activities. Instead the emphasis was on conditioning behavior at specific locations. Commerce, through data mining and profiling, was quick to implement the second generation, trying to overcome the limitations of the first. Computer-supported surveillance (the gambling industry led the way here), loyalty cards, credit card purchases, mobile phones etc. enable the harvesting of personal data on everybody, including not only those suspected of illegal activity, but also high rollers, frequent flyers, actual shoppers and potential customers at any number of lucrative locations.

It is hardly surprising that profit-oriented corporations were the first to adopt sophisticated profiling and data mining techniques. In its current form, individuals are awarded cash rebates or air miles when they present loyalty cards upon a purchase: what is this but a reward for good behavior? Bad behavior is punished; customers lose their benefits if they don't keep up their shopping momentum. Few people actually read the fine print before releasing their personal data; most are more concerned about their members-only savings than fair information practices. In other cases, the customer has no choice: it is impossible to return an item for a refund without releasing name, address and telephone number. Subsequently, databases mine the paper trails of everyone's lives, including all 'voluntarily' provided pieces of personal information as well as data from previously paper-based records that have been turned into electronic records (such as health records).

The combination of such private information with previously cumbersome-to-obtain public details (regarding lawsuits, liens, and so on) yields money-spinning profiles that can be repurposed and sold on. Unforeseen by the unsuspecting population at large, perhaps individuals' behavioral data is the long-awaited panacea for the problems of all sorts of secondary users. Insurance brokers and credit bureaux, that were previously crippled by the non-availability of such data, and employers who would like to learn more about their potential employees' physical and mental well-being,[5] are obvious customers. Of course, governments too can benefit from this new free-market in the exchange of personal data, and thereby advance from procedures for manually watching the deeds of society's members (such as through CCTV cameras) to automating the analysis of behavior.

At its beginning, this second generation appeared to depart from the previous panoptical identity architecture. Rather than explicitly trying to curb antisocial behavior through the presence of purely investigative technologies (such as a circular prison tower or CCTV cameras), or blatantly displaying the analytical nature of common technologies (such as loyalty cards) thereby scaring everyone into behaving in a socially acceptable manner, their true profiling and behavior-changing intentions were hidden behind seemingly beneficial and/or desirable outcomes for individual participants. But behind the scenes, U.K.'s Inland Revenue demands access to the records of supermarkets' loyalty cards in an effort to catch tax evaders;[4] the Pentagon purchases data on teenagers it can recruit into the military; and the Homeland Security Department pays for consumer information to help screen people at borders and to detect immigration fraud.[10]

However, unexpected consequences have come to light: more effectively targeted spam; tax audits of individuals who, according to their loyalty cards, live beyond their means; or identity theft based on individuals' electronic profiles. Consequently, personal information and its free disclosure is becoming a primary concern for many citizens. Increasingly, the actual investigative power and reach of second generation systems is becoming obvious to the general public. Privacy advocates and civil liberty groups are no longer the only ones alarmed. As the perceived drawbacks start to outweigh the benefits, the various promises are losing their appeal for the citizen. Weary consumers start to resent the constant demand for personal data, and even the ordinary homemaker begins to pay only with cash and provides fake names or telephone numbers for in-store rebates or returns. The effectiveness of the system is once again diminished. Similar to the previous generation, individuals manage to deceive the system, slip through the cracks, or decide not to comply with its data collection. Hence, the flaws of the first generation have reappeared in second generation systems. What is going on?

The use of this technology by governments is also being queried. Some critics claim that the ultimate hidden goal of governments is to create a modern panopticon, with politicians believing in a society in which the mere illusion of monitoring and control mechanisms is sufficient to stop those with criminal intentions: an emphasis on crime prevention over correction. However, for such a ploy to succeed, the illusion must be tied to a real threat. In the original model, the prisoners had to fear that there really was a guard behind the mesh screen; today's citizens must believe that CCTV cameras are actually genuine, and cross-border shoppers must expect that their purchasing data (invoices and credit card data) are available to customs agents. Equally important, the presence of surveillance systems must be directly connected to the likelihood of disciplinary action. For if no legal action typically results, anti-social individuals would never change their behavior. Clearly, the technologies used in generations one and two are failing to intimidate, and are becoming less effective in reducing shoplifting, pick-pocketing,

smuggling, speeding, terrorism, and parking violations, to name but a few. The punitive threat of technologies appears to be held back by limitations in two fundamental systemic properties: the cohesive integrity within the systems involved; and the interaction, or coupling, between them.

Highly cohesive systems focus on related sets of data and precise tasks, and are clearly desirable in terms of robustness, reliability, and understandability. Today's panopticons, however, display low cohesion. They are difficult to maintain, difficult to test, and even more difficult to understand. Take the justice system: it uses many often-unrelated sets of data, and relies heavily on records, photos and fingerprints that are kept on prior felons. Therefore, first-time offenders and those who have managed to stay out of the system have nothing to fear from it. As a result, policing is carried out with numerous different investigative activities based on a number of unrelated data sources. In an effort to increase its systems' cohesion, in Britain the government is finding excuses to justify the DNA testing and recording of large number of innocent citizens. Even schoolchildren are not exempt from its National DNA Database (NDNAD), the biggest DNA repository in the world. CODIS, the Combined DNA Index System funded by the FBI in the U.S. is second, followed by California's own state system. In terms of reliability, the punishment of non-criminal offences is also problematic, where not all wrongdoings are caught and penalized equally. While governments can identify car owners, for instance, through the use of license plates, they simply do not have the manpower to ensure that all illegally parked vehicles are ticketed, clamped or towed. As a result, many offenders go free. In the same way, not all cars or cargo containers that cross borders are searched for illegal substances, not all foreign visitors undergo a detailed criminal check, and guns used in violent crimes are rarely registered.

Furthermore, the data that are available are stored in departmental silos, and are not always directly coupled or connected. By and large, activities within the justice system are recorded and treated independently of each other. Individual database systems manage various categories of offence, and in most cases allow for little data flow between systems. Even when feedback loops do connect systems to each other (such as one database to another, or human agents to technological systems), updating the respective entries rarely happens in real-time. For instance, the viability of the FBI's Investigative Data Warehouse rests on a number of agencies that update their records, which at times occurs on a daily basis, at other times monthly or even quarterly.[9] The mills of justice grind exceeding slow. Naturally, the fact that in the meanwhile many offenders go unpunished both dramatically reduces any threat, and undermines the effectiveness of the fable of an all-seeing panopticon presented by the justice system.

In their debility, governments turn to newer technologies in the hope of higher cohesion, more data, more data sources, and for more coupling, and greater timeliness. In the meanwhile, false positives clog up the justice system. The objective of the government is not only to catch more delinquents and arrest fewer innocents, but also to increase the perceived punitive power of the state. But how to achieve these?

For indeed, new technologies are now emerging that increasingly permit the automatic capture of data, tightening the government's net, and allowing fewer lawbreakers to slip through. Backscatter X-ray, for instance, automates airport security checks to the point where every traveler can be frisked. The amount of detail in the data produced is staggering. Today's installations of backscatter X-rays can produce photo-quality images of body contours that leave little to the imagination. Under the criticism of turning passenger screening into passenger voyeurism, some airports have dumbed down image clarity with random noise added to the data, but only to a point where the technology still serves as a great deterrent to carrying weapons on one's person. CCTV Cameras with face-recognition can now automatically identify passers-by based on their eigenfaces and landmark features. Computerized monitoring can also look for particular items (suitcases or coats), and compare the conduct of one individual on camera to the behavior of a larger sample in the same environment to identify suspicious behavior. In other instances, RFID-enabled cash promises to close the loop on information related to all monetary transactions;[1] Nexus cards transmit details of individuals crossing the U.S.A./Canadian border. Cohesion is on the rise, and connecting these individual systems more directly is part of many national information policies (such as the USA Patriot Act, the UK Regulation of Investigative Powers Act). But still, the places where data may be captured are limited in number, and are often constrained to specific physical locations (such as border crossings); the panopticon is still not working perfectly. Dissidents can still escape detection.

Enter the third generation. The computing power of spy technology has been placed in the hands of private citizens. Essentially, the growing embeddedness of IT artifacts throughout our social landscape, and the increasingly active involvement of information systems and devices in everyone's lives, can substantially increase the area under surveillance, and do away with the need for more policemen. By outsourcing policing duties to the general population who are harnessing the investigative power of common technologies, the data density within our judiciary systems can be increased enormously. The ultimate public panopticon can be achieved by convincing the population to spy on itself. When live CCTV feeds become tied to geospatial applications on the Internet (such as Google Maps' highly detailed Street View feature), the elderly will no longer spy only on their local neighborhoods from behind lace curtains, they will be able to watch a much wider area online.

There are many much more effective personal devices that could be included in this architecture. Take mobile phones; they are everywhere, and their functionality continues to amaze. The convergence of cameras and phones was seen as the next killer application to replace the highly lucrative text messaging (SMS), with Multimedia messaging (MMS). Although MMS is generally considered a failure, cameras are still in phones and videos and photos are being recorded all the time. This omnipresence presents a new lens to the concept of the panopticon. Examples are in the recent instances of teacher-

baiting, in which students provoke and taunt their teachers to a breaking point. These classroom dramas, caught on camera phones, are then uploaded to popular video-sharing sites (such as YouTube.com) for all to see, often sparking discussions about the dismissal of the teacher in question. But fortunately, some schools already have cameras installed in their classrooms, too. Instances outside of the classroom involve similar e-evidence. Photos taken by bystanders on camera phones are regularly introduced into newsfeeds (such as the Tsunami of 2005 and the shootings at Virginia Tech in 2007). Coverage shot by citizen-reporters is frequently requested for court-cases (such as the London bombings of 2005). It was pure coincidence that a video camera was present at the Rodney King incident in 1991, but today one must suspect that all actions, legal or not, right or wrong, are likely to be caught on camera.

These examples illustrate another important change. No longer are we just looking at simple photographs, but at evidence that is widely shared through blogs, micro-blogs (such as Twitter), social networking sites (such as Facebook) and video-sharing sites (such as YouTube). Without these technologies, the phenomenon of teacher-baiting would not be nearly as popular. But it is not all anti-social. The cyber-mob can take the moral high ground. All it requires is a common technological platform to share e-evidence in order to police social behavior. In July 2005 a young woman was traveling with her lap dog on a South Korean subway train, when the dog was 'taken short' and defecated on the carriage floor.[7] A fellow passenger gave the woman a tissue, and she promptly cleaned up her pet, but left the mess on the floor. Angry passengers demanded she wipe it up; the woman rudely refused and left the compartment. A few elderly complainants on the train then did the job themselves. But the story didn't end there. One passenger had taken photographs of the drama with a mobile phone, and incensed, posted the pictures on the Internet. The story spread like wildfire and it wasn't long before the 'dog-poop' girl was identified, and her details broadcast on the Net. Consequently she and her family faced a barrage of abuse from 'netizen vigilantes,' and she was forced to terminate her education program.

The Internet and the mobile phone camera is a powerful combination. In this case it was a communal sense of indignation that sparked the witch-hunt. Think what could happen if people were paid to report any anti-social behavior they saw and recorded? Next, add a Global Positioning System to each mobile phone – this will soon be a legal requirement in Japan. Now suppose the longitude and latitude can be superimposed on any digital photograph along with a tamper proof time signal. Add on a checksum and digital certificate that guarantees the image has not been altered with the likes of Photoshop, include the abovementioned facial recognition features, and finally invite such images to be submitted as evidence in a court of law. By instantaneously e-mailing such a certified photograph (or video) from the mobile phone to the authorities of say anyone being illegally parked, the photographer could be paid a bounty, a flat amount or a percentage of the penalty to encourage catching offenders. Such practices are strongly reminiscent of the *Spitzels* of the former German Democratic Republic and of civil informants in China today – or indeed the 'Wanted: Dead or Alive' posters from the Wild West. The difference now is that the state can pay rewards directly and anonymously into the telephone account, and have the mobile phone payment system changed, allowing credit on an account to be withdrawn at post-offices. No more traffic wardens - we're all Stasi now!

But the payment needn't be monetary. Virtue is its own reward. Like in the 'dog-poop' case, if the authorities make it easy to report anti-social behavior, a suitably motivated general population will be lining up to hand over offenders. Under the banner of 'saving the planet', it is already commonly accepted as right and proper to police the carbon footprints of others, and by connecting personal technologies to the justice system, it would be easy turn in the eco-criminal that is your neighbor. We have come full circle, and are back with Jeremy Bentham and his assertion that the rightness of an action entirely depends on the value of its consequences. Smoking in a non-smoking designated area, using a mobile phone while driving, jaywalking, vandalism, littering, and a hundred and one other crimes and misdemeanors could be policed, and punished in this way.

But by then every honest citizen has become criminalized, with society itself as the prison, and each prisoner doubling up as a potential guard and bounty hunter. The state doesn't need to pay salaries to the jailers; it's all pay-by-results spying and sanctimonious reporting. At last, the ultimate panopticon, and it's coming soon to a neighborhood near you! C

**References:**

1. Angell, I. and Kietzmann, J. RFID and the end of cash? *Comm. ACM 49*, 12, (Dec. 2006) 90-96.
2. BBC (Aug. 24, 2009). "1,000 Cameras 'Solve One Crime.'" http://news.bbc.co.uk/2/hi/uk_news/england/london/8219022.stm.
3. Bentham, M. CCTV spy cameras will TALK in London *London Lite*, 2007; http://www.thisislondon.co.uk/news/article-23391487-details/CCTV+spy+cameras+will+TALK+in+London/article.do
4. Graham, B. George Orwell, Big Brother is watching your house. *Evening Standard*. http://www.thisislondon.co.uk/news/article-23391081-details/George+Orwell,+Big+Brother+is+watching+your+house/article.do
5. Hopegood, J. Taxman snoops on loyalty cards *Daily Mail, This is Money*, 1999; http://www.thisismoney.co.uk/tax-advice/article.html?in_article_id=385777&in_page_id=11&in_a_source=
6. Industry Canada. Why Do We Care About Privacy? Canada's Office of Consumer Affairs, ed., 2006. http://strategis.ic.gc.ca/epic/site/oca-bc.nsf/en/ca01360e.html
7. Kim, J. Subway fracas escalates into test of the Internet's power to shame. *The Washington Post*, 2005; http://washingtonpost.com/wp-dyn/content/article/2005/07/06/AR2005070601953.html
8. Magnes, T. Private speed controls in Graz (Austria). European Local Transport Information Service, 2007. http://www.eltis.org/PDF/generate_pdf.php?study_id=1323&lan=en&PHPSESSID=ce4b9e7971487f0f9e02251fc45fda44
9. McCullagh, D. Post-9/11 antiterror technology: A report card *Security*. ZDNet News, 2006; http://news.zdnet.com/2100-1009_22-6113064.html
10. Mohammed, A. and Kehaulani Goo, S. Government increasingly turning to data mining. *The Washington Post*, 2006. http://www.washingtonpost.com/wp-dyn/content/article/2006/06/14/AR2006061402063_pf.html

**Jan Kietzmann** (jan_kietzmann@sfu.ca) is an assistant professor in the Faculty of Business Administration at Simon Fraser University.

**Ian Angell** (i.angell@lse.ac.uk) is a professor in the Department of Management at the London School of Economics.