

Everyday Surveillance

ID cards, cameras and a database of ditties

SHUDDHABRATA SENGUPTA



At first glance, a city like Delhi is not one that you would associate with a tight mesh of surveillance. We don't (as yet) have surveillance cameras at every bus stop in the New Delhi area, as is the case, say, of the City in London, or much of lower Manhattan. But does this mean that we (in Indian cities) are invisible (or inaudible, or untraceable) to the apparatus of information gathering, or the matrix, or whatever you may like to call it, that links all the government, corporate and civic agencies that have an interest in keeping an eye on things?

As someone who has been following (somewhat perfunctorily) the growth of the surveillance industry in India, I have grown accustomed to tracking the slight shadows of data gatherers that lurk at the unlikeliest of places. I have gathered, over the last year, a few observations and notes, my banal and everyday log of surveillance on surveillance, that I would like to present here, and they are as follows:

There are very comprehensive plans being made for a massive 'citizen database' to be owned and operated by the state. For some reason (intra-governmental) this could not be done in sync with the recently conducted census, but census data will no doubt be used for building this database. This exercise will climax in various schemes, either NISHAN (National Identification System Home Affairs Network) or the INDIA CARD, by which all citizens will have to carry identity cards containing identifying photographs, all relevant infor-

mation (including legal records) about them, and biometric data (data about their body measurements, handprints etc.)

The Union Ministry of Home Affairs has commissioned Tata Consultancy Services (TCS), a software consultancy multinational based in India, to do a feasibility study for the National ID card scheme. The TCS report suggests that the whole exercise be made market friendly, and that the state actually make money out of it by selling information that it gathers about citizens to corporate bodies. This will no doubt be seen as a model mechanism of 'self-reliant' state control.

To find out more about NISHAN read the following news reports:

Dataquest Magazine: http://www.dqindia.com/content/top_stories/101022206.asp

The Hindustan Times: <http://www.hindustantimes.com/nonfram/170900/detFEA03.asp>

The other proposal – the INDIA Card Scheme – is put forward by a private Bangalore based company (Shonkh Technologies International Ltd.) which no doubt will be a major player in terms of making a bid for actually executing this scheme on an India-wide basis. To find out more about this, visit the Shonkh Technologies web site at <http://www.shonkh.com/indiacard.html>

In fact, the first instance of a comprehensive national computerised identity card system has been tried out in Thailand where it is now in operation. Pakistan has had a 'shanaqti card' (Identity Card) system for decades. All Pakistani citizens must carry the photo ID card which also states their religion. The hated 'passes' in Apartheid era South Africa were basically ID Cards that also mentioned 'race'. The genocide in Rwanda was facilitated by the recently introduced Identity Card system that helped distinguish between Hutus and Tutsis.

It is not always the industrialised West that takes quickest to the dissemination of high-tech surveillance schemes on a 'nationwide' basis. Modernising elites in the so-called 'Third World' are often better placed (due to lack of constitutional safeguards to privacy, or lack of awareness at the public level of privacy issues) to put in place 'technologies of mass surveillance'.

An identity card scheme may seem innocuous, but its implications are very dangerous. Apart from the fact that in India pogroms (the Anti-Sikh pogroms of 1984, for instance) have sometimes been administered with the help of electoral registers, and computerised ID card systems would make such exercises that much simpler and more efficient, there are other serious implications of a regime of national identity cards.

Information about each of us is scattered in various data banks. These could be police records, medical records, electoral registers, taxation records, etc. Their collation in a single database has devastating consequences. Let us imagine that we all have our NISHAN cards already:

The entries in one set of data can influence other, unrelated parameters. Let me give you a hypothetical example: a centralised electoral roll could register whether or not someone has voted in any electoral exercise. I, for instance, don't vote. If 'not voting' were ever to be rendered a disqualifying factor in any other circumstance – applying for a passport, a phone, a gas connection, a job – then my non-voting behaviour would show up, every time I did any of those other things. Suppose I go for a job interview, I am asked for my NISHAN/INDIA card, which I submit, it reveals that I have not voted. I get disqualified.

Naturally my objective record as a non-active citizen influences the decision. I don't get the job.

A huge invasion of privacy gets legitimised. Suppose I am HIV positive, and my medical records register that on my card. I need to rent a house. New regulations stipulate that all landlords have to have prospective tenants cross-checked at the local police station. They ask for my NISHAN card, run it across their machine that hooks up to the centralised database, and of course it reveals that I am HIV positive. The landlord, (perhaps the whole neighbourhood) and the police station know that I am HIV positive, I don't get to be the tenant they choose.

Consider that the Indian Constitution does not recognise the Right to Privacy as a fundamental right. Consider also that the state will (if this scheme gets under way) have the freedom to farm and manipulate enormous chunks of data about citizens. Consider also that those who will not get the cards (perhaps they are emigrants or refugees – the Bangladeshi *rickscha* puller, the Afghan auto *rickscha* driver) will now have to face considerable police harassment at day-to-day levels because they will not be able to produce their cards when they are stopped on the streets.

Identity cards already operate in Jammu & Kashmir and other border areas, where you can be stopped routinely and asked to produce them. Jammu & Kashmir has the distinction, incidentally, of being the one state of the Indian Union where there is also no mobile telephony (notice how the Bharti Telecom Ads on Television speak of "Himachal to Kanyakumari" and not the customarily alliterative, "Kashmir to Kanyakumari"), where long distance telephony is curtailed, and where Internet access has recently been redefined in the direction of non-existence following rising tension on the India-Pakistan Line of Control and the international border.

The situation on the ground in cities like Delhi and Mumbai is admittedly different, but only to a degree. In Mumbai there already exists a police scheme by which you have to produce a passport, or an identity card to surf in cyber cafés,¹ and there are serious proposals to extend this scheme to Delhi as well. This is being done, we are told, to protect minors from accessing unsavoury web sites, and in the interests of national security. Apart from this, some segments of the population in Delhi, such as rag pickers, are now being issued identification cards that they must carry with them at all times.

Identity cards are only one element in the apparatus of surveillance. Even more crucial are the sweeping powers of a battery of legal instruments ranging from the Prevention of Terrorism Ordinance (POTO) to the Information Technology Act and the Communications and Convergence Bill, which authorise a spectrum of state agencies to 'intercept communications' in the interests of state security. POTO is innovative to the extent that it criminalises the failure to furnish information by ordinary citizens very stringently, and allows for the drawing of 'adverse inferences' if a person accused under POTO refuses to voluntarily offer blood samples and furnish other biological samples when asked for. This presupposes that the administrative and technological apparatus necessary to create large-scale biological databases for reasons of state security already exists, or is in an advanced process of construction.

Typically, high-tech interventions in the area of surveillance are initiated with the pur-

pose of keeping a watch on potential terrorists and others labelled criminal. For example, a Prisoner Identification and Tracking System is already being implemented as a pilot project at the Cherrapalli prison in Hyderabad, Andhra Pradesh. The 150-acre prison houses over 3,000 inmates, and is the first prison in the country to experiment with this technology. The prison authorities have installed local positioning systems which provide real time information on the movements and whereabouts of the prisoner who has a label tagged on to him. If he removes the label, it triggers an alarm.

Very soon, genomic records, or electronic tags can find applications in workplaces – in offices, factories and public spaces. The high-tech surveillance industry actually sees India as one of the most lucrative potential markets with a growth potential of 25% in an industry that already has a turnover of close to US\$ 120 million per annum.² The highest demand is predicted for high-tech 'access control' systems – precisely of the kinds that are being tried out on the inmates of Cherrapalli prison (for a detailed industry report on Surveillance Equipment and the rising demand for it in India, go to <http://www.tradeport.org/ts/countries/india/isa/isar0019.html>).

Surveillance cameras are already making their entry into our lives at various major traffic intersections and in all of central New Delhi, as well as in banks, apartments, offices and industrial areas. If you couple pattern recognition systems on to video surveillance footage, then you have the surveillance camera meeting the identity card in a database somewhere in a mainframe computer. It is most likely that a very large number of people in cities will get caught in the crossfire between the huge arrays of data produced by 'citizen databases' and surveillance technologies.

Incidentally, the kind of people who sell surveillance equipment are also often the kind of people who sell torture equipment (electrical appliances) which go under the name of 'crime control' equipment. If you look hard enough on the Internet, you will find the same companies selling this kind of stuff in India, Turkey, Brazil, and other democracies.

Finally, I would like to mention the fact that the information gathering apparatus acts concretely and at the most everyday and intimate level.

If you want to know what a police identification form of a 'floating population' looks like, all you need is to download the marvellous form prepared by the Chandigarh Police at: http://chandigarhpolice.nic.in/vschandigarhpolice/b_form_4.pdf and see the meticulous detail with which it requires a beat constable to fill in data about *ricksha* pullers/auto *ricksha wallas/rehri* (handcart), *pheri* (itinerant vendors), *dhaba* (small eateries) *wallas/maids/malis* (gardeners) and labourers.

Similarly, the Delhi Police ("With You For You Always") also requires servants to be registered and verified, with the registration form containing details like "His/Her Favourite Ditty" and "His/Her Pet Words of Speech". This form can be downloaded at <http://delhipolice.nic.in/home/servant-f.htm>.

Somewhere, there are people in the Delhi Police who maintain a database of ditties.

On a slightly graver note, in the wake of the recent attack on the Indian Parliament, the apparatus of surveillance has now embraced every single e-mail that comes from Internet accounts in India. The report that details this extraordinary measure bears quotation at some length.

"The Intelligence Bureau (IB) has prepared a list of new keywords that are to be used to intercept mails emanating from IP addresses in India. Till now, the IB had concentrated more on e-mail IDs with reference to obvious giveaways such as Kashmir, Lashkar, Pakistan, Musharraf, etc. For example, an e-mail ID such as lashkar@hotmail.com should be under the surveillance of the IB. The IB has now gone further and prepared a new list of keywords used in the copy of mails that will be intercepted.

The system works like this: A software filters mails that repeatedly use the words that the IB has short-listed. The more obvious keywords would include Jaish, Kashmir, Lashkar. Others are attack, kill, rocket. Mails with repeated reference to Arab names will also be under surveillance.

Mails that carry names of Indian political leaders will also be under surveillance. However, the software can't decipher code words since they can be common words. Interestingly, the CIA is using the same software with a good success rate.

'The task of monitoring such mails is humungous. Hence, for now, we will be monitoring mails that have several references to the keywords that we have identified', says a senior IB official. According to the official: 'The IB is the only Indian intelligence agency that has the ability to intercept mails. None of the other agencies involved in investigations – the Delhi Police, the Central Bureau of Investigation (CBI), Research and Analysis Wing (RAW) – have the ability to intercept mails. Only the CIA has similar capabilities'.

Commenting on the issue of invasion of privacy of an individual, the official said: 'This exercise is similar to the secret cell phone tapping of suspects involved in *hawala* as well as cricket match-fixing, that was implemented by the Delhi Police. It met with a lot of success. The issue of intercepting mail is being done in the interest of national security'.

The official, however, also admitted that the exercise of intercepting mails would present a logistical nightmare given the huge mass of mails emanating from India".³

We can only hope that the logistics that inhibit a near total regime of surveillance continue to remain a nightmare, at least for a while.

NOTES

1. Leslie D'Monte, "Stop Cyber Surfer, where's your ID?" in *Zdnet India* (www.zdnetindia.com/news/features/stories/22533.html, 16 May 2001).
2. Neeraj Bhatnagar, *Industry Sector Analysis Report of Safety & Security Equipment in India* (Department of Commerce, US & Foreign Commercial Service and US Department of State, 1999).
3. *The Times of India*, 24 December 2001.

REFERENCES

- For an analysis of the politics of Privacy and Surveillance, go to the Privacy International web site at <http://www.privacyinternational.org/>
- For a good summary of the politics of online privacy issues, go to the Global Internet Liberty Campaign (GILC) web page on "Privacy and Human Rights" at <http://www.gilc.org/privacy/survey/>
- For an "India Country Report on Privacy Issues" at the GILC site, go to <http://www.gilc.org/privacy/survey/surveyak.html#India>