Smile: You are on Camera! The Rise of Participatory Surveillance

Pramod K. Nayar
The University of Hyderabad, India

Abstract
This essay uses the Unique Identification Number (UID) introduced recently in India to meditate upon the surveillance society. It opens with a discussion of identity and identification, arguing that identity cards and biometric data are forms of identification through which a society validates the claims of identity. In the second section it argues that biometric surveillance and data-collection reintroduce the body as the key component of human identity. In section three it makes a case of participatory surveillance where we all willingly subject ourselves to observation but are in turn ourselves observers in what is a new format of surveillance – diffused multiveillance.

[**Keywords**: identity, participatory surveillance, UID, biometric, camera, location]

One of the world's largest Internet search engines, Google, tells you quite cheerily:

> Google attempts to automatically detect your location and customize results based on that detected location. A location that's labeled "Auto-detected" is chosen based on the following factors:
>
> - Your IP address. (http://www.google.com/privacy_faq.html#toc-terms-ip)
> - Google Toolbar's My Location feature. If you have Google Toolbar installed and have the My Location feature (http://www.google.com/support/toolbar/bin/answer.py?answer=166104) enabled, your approximate location (if detected) will be used to customize your search results.

And what if you do not wish to be detected? Sorry – you have no choice in the matter, for Google is clear that:

> The customization of search results based on location is an important component of a consistent, high-quality search experience. Therefore, we haven't provided a way to turn off location customization, although we've made it easy for you to set your own location or to customize using a general location as broad as the country that matches your local domain.

In other words, it is entirely in our interest that we are tracked by Google's vast machinery – so that we can get better search results. Facebook, the world's most popular social networking site, developed a 'face recognition technology'. It would compile user profile photographs to prepare a biometric database for this purpose – and to match 'faces'. But few users were aware of this move. It ran into controversy when organizations such as the Electronic Privacy Information Center (www.epic.org) filed cases with the Federal Trade Commission in June 2011 (for reports see Raphael 2011). You are photographed by the CCTVs in supermarkets. Your PC records every stroke on the keyboard. Amazon.com

Rupkatha Journal on Interdisciplinary Studies in Humanities (ISSN 0975—2935), Vol.3 No.3, 2011.
Ed. Tirtha Prasad Mukhopadhyay
URL of the Issue: http://rupkatha.com/v3n3.php
URL of the article: http://rupkatha.com/V3/n3/05_Participatory_Surveillance.pdf
Kolkata, India. © www.rupkatha.com

helpfully offers advice: 'those who bought this book also bought…' Smart air-conditioners set their controls after measuring the temperature and humidity in the room, and the presence/absence of people/bodies. GPS and GPRS trackers in cellphones relay data about your exact location. And now we have the Unique Identification Number (UID), India's biometric identity card. Nomadic eyeballs (cameras), traffic cameras, face/palm recognition software in your laptop … the list of places and acts when one is visualized and rendered into some databank or the other is endless. We watch, even as we are being watched. Welcome to the age of surveillance.

A cursory glance at an online etymological dictionary yields interesting results for the word 'surveillance'. First entering usage in 1802, from the French, surveillance means 'oversight, supervision, a watch', a noun of action from 'surveiller', and derived from 'sur-' ('over') and 'veiller' ('to watch'), originating from the Latinate 'vigilare' ('watchful'). There is a suggestion here of an observation platform – of somebody 'over' or 'above' who keeps a vigil over us.

This sense of the term 'surveillance', I argue towards the last section of my essay, is no longer valid. The nature and structure of surveillance has changed considerably, even though the panoptical model does exist alongside. But before addressing this change in the modes of surveillance, it is necessary to map the larger contours of our surveillance society. I use the Unique Identification Number (the UID) launched with much fanfare and hope by the Government of India in 2009-10 (and the process is now underway) as an immediate context for the meditation here, but the essay is not restricted to the Aadhaar/UID issue. It is too early to see where UID is headed, given the logistic and technological task it has set itself. However, using the UID as a point of departure, this essay meditates on the nature of our observed and observer lives in the age of the information state and in the condition of perpetual surveillance.

Identity, Identification, Surveillance

In a surveillance society we are not seeking identity as much as an *authentication of a claimed identity*. ID cards are not meant to identify you, but to validate your claim that you are who you *say* you are. ID cards reduce you to a set of interpretable data. In other words in a surveillance society identity is not acceptable unless and until you can prove it and the proof, in the form of some document or the other, is *accepted* by a designated authority. Thus a bus pass issued to a student is not about Mr X or Ms Y, but identifies him and her as an authentic student entitled to a discounted fare. We therefore need to understand that surveillance societies are working not with a concept of identity (which is individualized, and embodied in the person) but with *identification*. Identity is how I perceive and describe myself ('I am…'), it is a narrative that I tell myself. Identification, on the other hand, is about an external validation of this narrative: 'You are…'. This is an important distinction, for while my identity need not be validated for myself, it requires validation for existing in the *world*.[1] I need to be accepted and identified for/as what I perceive, describe and represent as my-self.

As David Lyon points out, identification and verification are ways of recognizing someone (2009: 115). A surveillance society seeks to identify you *from* a large mass of people. ID cards are markers therefore not only of embodied identity or personality but of your distinctiveness *from* somebody else. Identification is the process of isolating one individual from a group.

The irony of this process of identification should not be lost on us. While we complain that we are becoming more and more self-involved and losing a sense of the collective/communitarian (a charge leveled against online lives in particular) technologies of surveillance and identification, often state-sponsored, emphasize the individualism and singularity of individuals. Social theorist Chris Jenks sub-titled one of his books, 'the fragmentation of the social.' Surveillance, it might be contended, calls for this fragmentation, to capture individuals within a set of data unconnected and isolated from anybody else. Your UID makes you *unique*. We are made even more conscious of our-selves here: this fingerprint, iris-scan, is *me*. My sense of self, my personhood is something I can comprehend better when I see a card inscribed with my more intimate data.

UIDA claims the Aadhaar card ensures that the underprivileged get the full benefits of the state's welfare schemes. Thus the dominant discourse here is welfare. As the 'Strategy Overview' document of the UIDA states:

> In India, an inability to prove identity is one of the biggest barriers preventing the poor from accessing benefits and subsidies …
>
> A clear identity number would also transform the delivery of social welfare programs by making them more inclusive of communities now cut off from such benefits due to their lack of identification. It would enable the government to shift from indirect to direct benefits, and help verify whether the intended beneficiaries actually receive funds/subsidies. A single, universal identity number will also be transformational in eliminating fraud and duplicate identities, since individuals will no longer be able to represent themselves differently to different agencies. This will result in significant savings to the state exchequer. (*Strategy Overview*

http://uidai.gov.in/UID_PDF/Front_Page_Articles/Documents/Strategy_Overveiw-001.pdf, 1)

It guarantees 'identity, not citizenship' (2), as the document takes some pains to emphasize.

This discourse of state concern and welfare is in contrast with countries like the USA where the discourse of identification that dominates such technologies is mainly of securitization: we are doing this to secure our borders. Yet there is the veiled security rhetoric at work in Aadhaar as well:

> For governments and individuals alike, strong identity for residents has real economic value. While weak identity systems cause the individual to miss out on benefits and services, it also makes it difficult for the government to account for money and resource flows across a country. In addition, it complicates government efforts to account for residents during emergencies and security threats. (*Strategy Overview* 6)

There are several issues thrown up by these claims. First, there is the implicit assumption that biometric profiling can enable the state to separate from the genuine applicants for welfare and the fake/false ones. Related to this is the assumption that the mobility of the people can be monitored across the country – an assumption that clearly indicates a surveillance mechanism. Second is the assumption that biometric identification can serve as a mechanism of prevention. Third, the data collected can be used by the government to monitor beneficiaries but also fake identities and criminals (a 'watch list' will be prepared, says the document, of individuals who try to apply for a second UID). It can function, therefore, as a mode of social ordering and categorization.

The Body Returns

Biometric IDs are the culmination of a surveillance culture where the body returns as the key figure in any identification. From fingerprinting to full-face photographs that passport and visa authorities insist on, the body has always documented, measured, recorded and compiled into data somewhere. The UID captures fingerprints, the face in its entirety – called 'face detection'—and the iris patterns. The UIDA informs us:

> The iris is the coloured ring around the pupil of every human being and like a snowflake, no two are alike. Each are [sic] unique in their own way, exhibiting a distinctive pattern that forms randomly in utero. The iris is a muscle that regulates the size of the pupil, controlling the amount of light that enters the eye.

(http://uidai.gov.in/index.php?option=com_content&view=article&id=168&Itemid=165)

On the one hand biometrics can be seen as a response to the increased 'dematerialization' of the human (where we are merely online creatures, with even social interactions 'reduced' to electronic communications and no face-to-face meetings): the body returns as the foundation of the human.

On the other, it could be argued that the human consists not only of the body but several other factors, including her/his psychology (called 'personality' in common parlance). Am I reducible to my iris or fingerprint? Or is there more to me?

Another way of treating UID's biometric data-collection is to see the material body being rendered into numbers (what has been called a 'mathematization' or 'informatization' of bodies). Located somewhere between an emphasis on the material body (in the form of unique fingerprints, iris-prints, etc) and the numerical imperative (the prints being converted into mathematical data), biometrics is this strange condition of body-technics.

UID is an instance of what Eugene Thacker calls 'biomedia', the 'technical recontextualization of biological components and processes', where the body is a medium and *where the media themselves are indistinguishable from the biological body* (Thacker 2004: 13) The body here needs to be understood in two ways – as a biological body, a species body *and* as a body that is 'compiled' through modes of visualization, modeling and datasets. It is flesh made into data, even as the data can be, when passed through appropriate scanners and devices, called upon to 'produce' a body. The individual is now not simply a mass of flesh, bones, fluids and nerves. S/he is all this plus a dataset which encodes all this and 'reveals' it all when passed through a scanner. In the information age I am *My Body + My biometric data*. My body *is* the data, just as the data on the smart card is *me*, each codes for the other. My body is the medium through which the necessary data flows into the card. We now need to see the bodily/biological identity of a person as indistinguishable from the visual, digital media of and on the card. I *am* biomedia, where biology, algorithms of the biometric data-set and the visual 'files' all merge to define 'Me'. The ontological status of the body is rendered into media and the media can be made to 'manifest' a body resulting in a flesh-data assemblage, a techno-ontology.

Interestingly, identity and identification has for a long time relied almost exclusively on the body's *surface*: fingerprint, face recognition, gait recognition, etc. With newer technologies identity issues have gone deeper, literally. Increasingly 'invasive' procedures seek to penetrate the body in order to establish identity – DNA fingerprinting, iris scans, brain mapping and blood sampling, all dredge deeper into the body to find more evidence for identification.

That biological identification of the kind biometrics relies upon is not infallible is something its critics have pointed out. Thus bodily features might change with age, lifestyle and environment: in those who perform hard labour with their bodies, for instance. Biometric databasing does not account for environment or ecology of individuals. Joseph N. Pato and Lynette I. Millett of the Whither Biometrics Committee, the National Research Council, USA, write in *Biometric Recognition: Challenges and Opportunities*:

> Biometric characteristics and the information captured by biometric systems may be affected by changes in age, environment, disease, stress, occupational factors, training and prompting, intentional alterations, sociocultural aspects of the situation in which the presentation occurs, changes in human interface with the system, and so on. As a result, each interaction of the individual with the system (at enrollment, identification, and so on) will be associated with different biometric information. Individuals attempting to thwart recognition for one reason or another also contribute to the inherent uncertainty in biometric systems.
>
> (http://www.nap.edu/openbook.php?record_id=12720&page=3)

Biometric States and Databorders

Aadhar, the UID, will be issued 'for all residents' (http://uidai.gov.in/index.php?option=com_content&view=article&id=57&Itemid=105).. The entitlement is defined thus: 'An individual who is a resident in India and satisfies the verification process laid down by the UIDAI can get an Aadhaar' (http://uidai.gov.in/index.php?option=com_content&view=article&id=59&Itemid=107). It will be 'recognised and accepted across the country' (http://uidai.gov.in/index.php?option=com_content&view=article&id=58&Itemid=106). All this is fascinating. What is significant is that the state's borders are converted into something immaterial, as a dataset. Only 'residents' are entitled to a UID. Conversely, a set of data defines who is resident within the sovereign state of India. Migrants, refugees and the 'undesirables' within and outside the state borders can be profiled as 'high-risk' groups through this, resulting in one more technology of social control. A state's borders are, as Javier Duran argues, now 'virtual' (2010). They are encoded in the form of data on the card that you carry so that when you seek to cross territorial borders the card sends out a signal that you are doing so. The state's borders, in other words, are what you also *carry* in your biometric data on the smart card – a mobile border. It moves with you, and determines where and how your body moves.

The body is now monitor-able as it moves across borders. The *Strategy Overview* document states: 'The UID will also give migrants mobility of identity' (4). What this also implies is that migrants can be *tracked*. What is possible now is the tracking of all mobilities so that conditions of legitimate and illegitimate mobility can be imposed. Like passport controls at borders, biometric data will now determine whether you can cross a territorial border. The legitimacy of border-crossing is *within* your body, your iris, your fingerprint, your DNA. External borders of states are to be reflected in the biometric borders – also the border between licit and illicit, legal and illegitimate – of the individual. The biometric border, writes Louise Amoore,

> is the portable border par excellence, carried by mobile bodies at the very same time as it is deployed to divide bodies at international boundaries, airports, railway stations, on subways or city streets, in the office or the neighbourhood (2006: 338)

It is quite interesting that in an age when more people travel than ever before and globalization itself thrives on such flows, states introduce modes of monitoring these mobilities. As Mark Salter has shown in his analysis of the security measures in the USA, the mobility of some individuals is perceived as a major threat, and therefore the monitoring of *all* mobile bodies is made inevitable (2004: 78-9). The data your card's chip carries is literally a databorder – the zeroes and ones that legitimize mobility in biometric states.

In such an information state it is the database that one must worry about: who has access and what might it be used for? We are assured that

> The UIDAI envisions a balance between 'privacy and purpose' when it comes to the information it collects on residents. The agencies may store the information of residents they enrol if they are authorized to do so, but they will not have access to the information in the UID database. The UIDAI will answer requests to authenticate identity only through a 'Yes' or 'No' response (*Strategy Overview* 4)

In what is surely an elision, the *Demographic Data Standards and Verification procedure (DDSVP) Committee Report* of the UIDA mentions that the UIDA

> proposes to create a platform to first collect the identity details and then to perform authentication that can be used by several government and commercial service providers. (4)

It does not specify who/what these commercial service providers are. Data stored in such databanks offers the potential of monitoring various individuals in multiple domains, a process now known as 'dataveillance'.

There is another component that does not quite get spelt out in the UIDA discourse. Aadhaar, the UIDA claims, is *not* mandatory. On the other hand it repeatedly announces that possessing a UID would benefit the poor and underprivileged to access the state's welfare schemes such as the Public Distribution System (PDS. See the document 'Envisioning a role for Aadhaar in the Public Distribution System,' http://uidai.gov.in/UID_PDF/Working_Papers/Circulated_Aadhaar_PDS_Note.pdf). If the UID is voluntary then it implies that a person who refuses to be biometrically registered will *not* have access to the state's resources. *The onus is on the individual to register, but not on the state to ensure that the resources do reach individuals even if they have not registered.* What is also implicit is that the UID is not only about belonging and being identified but it is also about citizenship rights which now are not automatic but demand validation through biometric data registering.

Issues of privacy pervade all debates about ID card processes and dataveillance. While states assure that the individual's right to privacy will be ensured, this remains a tricky issue. The right to privacy only means that the state will not share the information once it had collected it. It does not mean that the *individual* can refuse the right to share the information.

Participatory Surveillance

After 9/11 the US government, under the aegis of the Bureau of Justice Assistance, Office of Justice Programs, prepared a *Citizens' Preparedness Guide* (2002). Page 2 of this document calls upon Americans to:

> **Be aware.** Get to know your neighbors at home and while traveling. Be on the lookout for suspicious activities such as unusual conduct in your neighborhood, in your workplace, or while traveling. Learn to spot suspicious packages, luggage, or mail abandoned in a crowded place like an office building, an airport, a school, or a shopping center.
>
> (http://www.princegeorgescountymd.gov/oem/PDFs/familycitizenplan.pdf)

USA Today ran a feature 'Here's what to do if you're hijacked,' in which an expert on terrorist attacks suggested:

> You want to take a good look at who's getting on board. Do your own screening and profiling. You want to look into their eyes. You can tell a lot about people by looking in their eyes. Are they shifty? Are they nervous? (qtd. in Salter 79-80).

What exactly is at work here? The answer is fairly simply: there is a shift in the nature of surveillance itself.

We live in an age when our most consistent monitors are ourselves. We are called upon to monitor our blood pressure, check for lumps in breasts, and keep an eye on the blood sugar levels. With the medicalization of everyday life and easy technological devices that make this kind of self-monitoring easy, we surveill ourselves, participating in the general surveillance society processes. In *participatory surveillance*, as seen in the *Citizens' Preparedness Guide*, we also agree to keep an eye on neighbours and 'suspicious objects' at public places (passengers at airports or railway stations are exhorted to report any such objects to the police personnel). Thus we place ourselves under observation but are also part of the surveillance society in that we constitute a part of the *observing* team when we monitor others' behaviour.

Multiveillance is my term for the many layers of surveillance we *willingly* subject ourselves and others to. Winifred Poster, from whose essay on multi-surveillance I develop this portmanteau term (thereby adding to the already vast field of neologisms), has proposed that, in the case of call centres in India rather than 'a single actor model of technological agency, this framework widens the lense [sic] from just managers, to uncover an entire web of actors directly involved in the day to day operations of Indian call centers – technology vendors, outsourcing clients, American consumers, Indian shopfloor supervisors, and Indian employees … *each of these actors participate in their own independent surveillance of all the others through ICTs.* (2011: 869, emphasis in original)

Thus every actor places somebody else under surveillance so that we see a horizontal rather than a panoptical/overview model, which is hierarchic and spatially top-down. In multiveillance everybody reports on everybody/anybody else. Unlike in a traditional surveillance society where the state organizes this 'observation' of its citizens, in contemporary times, *citizens monitor each other.*

In a multiveillance society citizens observe each other to see who is not quite a citizen. This makes multiveillance a diffused or *dispersed surveillance system* where (i) information is gathered from multiple sources (ii) a connected network of eyeballs collates information and continuously feeds it into large databases. Each of us observing others acts as a node in this dispersed surveillance system, and thus constitutes a part of its network, even though we do not connect directly with other such nodes/eyeballs. Think of buses and vehicles that announce 'if I am driving badly, please call 1234567'. The system collates information from other road users who call the number about the vehicle/driver. The people who do call do not know each other, but collectively, in their dispersed ways, contribute to a data of information about the vehicle.

What we need to envisage is a system where different components of this diffused network do not always communicate with each other, each 'node' or eyeball sends in data into databanks, from which further data is transacted. When you use your ATM card, the information about that particular transaction is fed into the bank's central database which then documents your bank account *but also* the amount of cash left in the particular machine (and thus determines if the cash needs to be replenished). One act therefore does at least two related and yet independent info-gathering acts. Both bits of information are transmitted to different databases.

One of the features of biometric IDs, Louise Amoore argues, is that it fixes people's identities so as to predict their behavior and to prevent any unacceptable ones (339-40). Passport controls at airports, we know, are under pressure to carefully look at the individual seeking entry into a state. Risk identification is central to the process of scrutiny at borders. The UID, like all biometric datasets, can be used to identify 'risk categories' among the visitors, or residents. In the USA it is precisely this kind of risk profiling – directed, as expected after 9/11, against Arabs and Muslims, but also blacks – that has attracted criticism from civil liberties advocates. But the shift in thinking about surveillance here lies in the call to all citizens to watch the others.

*

Participatory multiveillance is here to stay, as more and more of the state relies on the gathering and classifying of information. This essay has only touched upon some features of this information state. Much more on the ethics of datagathering, datasharing and data-use needs to be addressed. And, to make one final proposition, this is a task that must be taken up not only by communications scholars but by the humanities, since within these dispersed surveillance societies the definitions of who counts as human is at stake.

So smile - You are On *My* Camera!

Note

[1] In Daniel Defoe's classic eighteenth century novel, *Robinson Crusoe* (1719), Crusoe is happy to meet another human being, Friday. The happiness is not because hereafter he (Crusoe) will not be alone. Rather it is because this another human being validates Crusoe's identity. Friday is trained to address Crusoe as 'master'. It is when the other human addresses Crusoe that Crusoe's identity is *identified*, recognized and validated.

References

Amoore, Louise. 'Biometric Borders: Governing Mobilities in the War on Terror,' *Political Geography* 25 (2006): 336-351.

Bureau of Justice Assistance, Office of Justice Programs. *Citizens' Preparedness Guide*. Washington, DC: Office of Justice Programs, 2002. http://www.princegeorgescountymd.gov/oem/PDFs/familycitizenplan.pdf.

Demographic Data Standards and Verification Committee. *Demographic Data Standards and Verification Committee Report*. New Delhi: UIDA, 2009. http://uidai.gov.in/UID_PDF/Committees/UID_DDSVP_Committee_Report_v1.0.pdf.

Duran, Javier. 'Virtual Borders, Data Aliens, and Bare Bodies: Culture, Securitization, and the Biometric State,' *Journal of Borderlands Studies* 25.3/4 (2010): 219-230.

Jenks, Chris. *Subculture: The Fragmentation of the Social*. London: Sage, 2005.

Lyon, David. *Identifying Citizens: ID Cards as Surveillance*. Cambridge: Polity, 2009.

Poster, Winifred R. 'Emotion Detectors, Answering Machines, and e-Unions: Multi-Surveillances in the Global Interactive Service Industry,' *American Behavioral Scientist* 55.7 (2011) 868-901.

Raphael, JR. 'Facebook Facial Recognition: New Technology, Familiar Problem,' *PC World* 9 June 2011. http://www.pcworld.com/article/229967/facebook_facial_recognition_new_technology_familiar_problem.html. 29 June 2011.

Ross, James C. 'Biometrics: Intersecting Borders and Bodies in Liberal Bionetwork States,' *Journal of Borderlands Studies* 22.2 (2007): 77-96.

Salter, Mark B. 'Passports, Mobility, and Security: How Smart can the Border be?,' *International Studies Perspectives* 5 (2004): 71-91.

Thacker, Eugene. *Biomedia*. Minneapolis: U of Minnesota P, 2004.

Unique Identification Authority of India, Planning Commission, Govt. of India. *UIDAI Strategy Overview: Creating A Unique Identity Number For Every Resident In India*. New Delhi: UIDA, 2010. http://uidai.gov.in/UID_PDF/Front_Page_Articles/Documents/Strategy_Overveiw-001.pdf.

Pramod K. Nayar *teaches at the Department of English, University of Hyderabad, India. His recent publications include States of Sentiment: Exploring the Cultures of Emotion (Orient BlackSwan 2011), An Introduction to New Media and Cybercultures (Wiley-Blackwell 2010), Postcolonialism: A Guide for the Perplexed (Continuum 2010), Packaging Life: Cultures of the Everyday (Sage 2009), Seeing Stars: Spectacle, Society and Celebrity Culture (Sage 2009), English Writing and India, 1600-1920: Colonizing Aesthetics (Routledge, 2008), among others. His forthcoming books include Digital Cool: Life in the Age of New Media (Orient BlackSwan), Writing Wrongs: The Cultural Construction of Human Rights (Routledge India) and Colonial Voices: The Discourses of Empire (Wiley-Blackwell).*