Gendering surveillance: A cautionary tale from India and Sri Lanka

Monday 18 June 2018, by Cat's Eye (Date first published: 13 June 2018).

The Government of Sri Lanka had planned, that effective from January 2018, all Sri Lankan citizens be required to carry a 'smart' e-NIC with biometric details (frontal facial photograph, fingerprints, iris scan), details of profession, address, phone numbers, date of birth, email and civil status. This e-NIC would also embed 'family tree' data including full names of parents and siblings, their dates of birth and NIC numbers.1

According to the Government the data is to gather information towards "efficient service delivery". What it would deliver, as the Indian Supreme Court ruled in the case of the Indian Unique Identification Number, is a gross infringement of privacy as well as vulnerability to data hacking. [1] How is an electronic identity card an infringement on privacy? It is not unreasonable to speculate that the e-NIC could be about quick, smart surveillance by the state. When swiped and checked in real time against a centralised database, the e-NIC will enable the state to digitally tag and track not only the 'citizen of interest' (including his/her financial transactions, property ownership, income tax file nos, etc.) but also his/her family members.

Therefore the proposed e-NIC goes well beyond the individual information contained in the current NIC cards we carry. Coupled with the intent declared recently by the SL government to introduce a Radio Frequency Identification (RFID) system to new vehicle license plates which will enable police to monitor vehicle movement, we are fast moving into an era of smart surveillance which operates by stealth.

Surveillance and 'women's safety'

Feminists have called attention to how such smart surveillance is citizen management in a new guise. Surveillance (parental, social, cultural) is a tried and tested tool of control of women, and the surveillance of women's lives is an age-old tradition across all cultures albeit in different forms.

Women have to answer to their families and communities about their movements – from "Where are you going?", "Who are you going with?", "What time will you come back home?" all the way to "When are you getting married?", "When are you going to have children?"

These so-called questions of 'concern' are only too familiar to most women. However innocent, these are normalised routines of surveillance and regulation of cultural norms, often in the guise of care and concern for women's safety and well-being.

While women can choose to evade such questions, surveillance devices such as e-NICs and RFID enable much more powerful entities than parents or curious relatives to know exactly where an individual is, at what time and at what place.

The normalisation of surveillance in this way is tied up with the idea that 'home' and 'family' are the ultimate 'safe-spaces' for women, and that families and communities know what's best for women. In

contrast, we know that this is rarely true.

There has never been a proven correlation between community/family control and a woman's actual safety. In fact, many women face violence and exploitation at the hands of their families and communities; home is often the site of prolonged physical, emotional or psychological violence against women. And yet, often, family and community control are seen as normal and healthy.

With the advancement of technology, the surveillance of women by their families will be complemented by, and even taken over, by the state in a manner which makes the line between family/community surveillance and State-surveillance increasingly blurred. When this happens we risk making the State's system of surveillance itself the subject of attention rather than the individual perpetrators of crimes against women.

Recently, the University Grants Commission (UGC) together with the Information and Communication Technology Agency (ICTA) launched a safety app that students and university staff can use to alert authorities such as marshals and university administration in case of ragging or sexual harassment and threat.

Cat's Eye welcomes this move if it works as a deterrent against ragging and sexual harassment. But we also strike a cautionary note based on an interesting study done in India which examined so-called 'women's safety apps' such as 'Raksha', launched by the BJP Government in 2014. The study (Gendering Surveillance, The Internet Democracy Project (Kovacs and Ranganathan 2017) questioned the functions and the premise upon which such apps worked.

It looked at how apps worked with personal data, and how the safety functions of these apps were disseminating personal data (such as location) to third-parties, like members of your family or even the state, via institutions like the police. It observed that none of the apps seemed to engage with existing research on violence against women, or actual national crime data.

For example, most of the apps work on the premise of making public spaces 'safer' for women, when recent data shows that less than 6% of rapes in India are stranger rapes. The UGC-ICTA app is only for University use, and the UGC and Universities will, hopefully, use the data appropriately and sensitively. But apps that track a person inevitably pose the question "Are you safe when the data about you is not safe?"

The problem is that many of us have consented to be tracked this way. Each time we download an app and decide to use it, each time we use our smart phone, we are trackable. So why the fuss, you may ask. Is this not a mere extension of the tracking devices already in use?

For instance, any clothing store in urban areas already has radio frequency identification of its clothes as a precaution against shoplifting. From tracking objects RFID is now used in the West regularly to track livestock and ex-prisoners on parole.

We have to be worried about our own collusion with the tech companies and social media platforms (such as Facebook that got caught recently selling personal data) which in turn collude with media agencies and lobbyists, bureaucrats, political parties and government. As the Facebook saga recently showed, we then become the target of propaganda and fake news based on the data gathered from us.

Biometric data

Biometric data is a key buzz-term in the world of tech-related solutions. The data gathered goes into the formation of citizen databases. Why should this be a matter for alarm?

First, Cat's Eye would like to provide a reminder to us all that the 'measuring' of bodies is a concept with a dark colonial past.

Native bodies from the colonies were studied and documented as 'specimens' (even modern-day museums in Britain showcase non-Western peoples in such a way), considered odd and 'non' normative. The normative, of course, being the body of the white man.

Native women from colonies in the African continent were famously paraded in front of white audiences in Britain, where one was supposed to look at her wide hips and large bottom with a suitable mixture of awe, fear and disgust (remember Sarah Baartman?) [2].

Modern-day body-scanning technologies in airports, for example, are actually no different. They are designed to recognise cis-gender (identifying with the gender you are assigned at birth) white bodies as 'the norm'. Therefore they flag other types of bodies as suspicious. Naturally matted or kinky hair? You could set off the alarm! Or perhaps you are an intersex person? Then you better watch out for those machines!

This is where privacy and the right to be who you want to be comes in. Can these technologies capture the complexities and varied experiences of people? How can they – when the power to design these technologies continue to be concentrated among an exclusive, homogenous circle of people: typically male, first-world and their counterparts in the rest of the world. And will technology keep women safe, in an environment where it is increasingly used by state and corporations to observe, manipulate, surveil, discipline and control?

(The Cat's Eye column is written by an independent collective of feminists, offering an alternative feminist gaze on current affairs in Sri Lanka and beyond.)

P.S.

Daily FT
http://www.ft.lk/opinion/Gendering-surveillance--A-cautionary-tale/14-657076

Footnotes

[1] Indian Supreme Court ruled in favour of 'the right to privacy' as a fundamental human rights in Aug 2017; many mainstream media outlets such as the BBC carried reports on this

[2] Sarah Baartman was a South African Khoikhoi woman who, due to her large buttocks, was exhibited as a freak show attraction in 19th-century Europe under the name 'Hottentot Venus'