Five New Ways In Which The Government Is Spying On You

From CCTVs watching your every move to the government monitoring your social media profiles, Big Brother keeps getting bigger. Here are some of the latest developments that should worry you.

Vitaly Nevar via Getty Images

It's no secret that the government snoops on citizens. But over the past few years, privacy advocates have been struggling to keep up with the sheer number of ways in which this is now done, thanks to technological advances. The assembly of a surveillance state is helped by a number of willing private companies, and today, there are discussions about having AI systems watch CCTV footage, while building 360-degree profiles from our different social media profiles on Facebook, Twitter, and Instagram.

Some plans are limited to specific states, or particular agencies, while others are more national in their scope. And new projects are being developed and implemented at a worrying rate, even as the government drags its feet on actually implementing the Draft Data Protection bill. Here are five of the latest developments in government surveillance that should have you worried about where things are headed.

Facebook, Twitter and Instagram accounts of students should connect to the HRD Ministry

A circular from R Subrahmanyam, Secretary, Ministry of Human Resource Development, sent to the heads of all Higher Educational Institutions (HEIs) earlier this month makes it clear that the government is interested in what students post on their social media accounts. The letter, which has been accessed by *HuffPost India*, states that the objective behind this demand is to share the achievements of HEIs through social media.

> **For the latest news and more, follow HuffPost India on Twitter, Facebook, and subscribe to our newsletter.**

The note asks HEIs to name a faculty or non-faculty member as the Social Media Champion (SMC) of the institution, with the job of opening and operating Facebook, Instagram and Twitter accounts for the institution, and connecting these to MHRD accounts. The SMC must also connect all students' social accounts with the institution and the MHRD.

This would perhaps be less concerning if the government also didn't have a history of reprisals against people for their social media posts, often using a law that has already been struck down. Earlier this year, a Kashmiri student was arrested for a social media post from 2012, which he wrote when he was 12 years old. Soon after, in Manipur, the BJP went to great lengths to take action against a student for a Facebook post. In Jharkhand, a Facebook post led to a professor's arrest. In Manipur again, a journalist was arrested and charged under NSA for uploading a Facebook video in which he criticised Prime Minister Narendra Modi and the state government. With so many examples, it's easy to understand

why people might be suspicious about the government's attempts to get students to connect their social media accounts.

Monitoring of mobile phones, landlines and Internet traffic

On July 4, responding to a question in the Rajya Sabha about a central monitoring system for mobiles, landlines and Internet users in the country, IT minister Ravi Shankar Prasad confirmed that the government has a system to monitor all these forms of communication. "At present, monitoring of Internet traffic through Internet Service Providers is being done through Internet Monitoring System which is under consideration for integration with Centralised Montioring System," Prasad said.

According to Prasad's reply, there is a Centralised Monitoring System (CMS), and 21 Regional Monitoring Centres, which have been operationalized all over the country.

The CMS is used to automate interception orders from law enforcement agencies to telecom providers. It will also allow for the electronic provisioning of targets without any manual intervention needed from the phone companies. It will also be able to continue interception and monitoring even if the target is roaming anywhere in the country.

The idea behind the CMS is not new—it was approved as far back as 2011. It is, however, a widespread and important system, and the fact that it seems to have dropped off the radar to the point where MPs need to ask about its existence is worrying, since the potential for its misuse is high, particularly with no safeguards in the form of a strong data protection and privacy law.

There's CCTV watching your children

State governments aren't sitting by the sidelines and watching the centre watch you either. The AAP government in Delhi has now started installing CCTV cameras in schools, ostensibly to prevent crimes and make

children safer. It has started with a school in Lajpat Nagar, but PTI reported that over 1,000 schools are supposed to be equipped with CCTV cameras by November. There is also a project to install CCTV cameras all across Delhi.

Parents will be able to access a live feed through an app on their phones. The idea is that the cameras will be used to collect evidence, and also act as a tool for deterrence. However, the privacy implications of capturing children on camera haven't been addressed by the government. Also, although Kejriwal said that this step was taken because of perverted elements in society, he does not acknowledge that in the process, he's also putting live feeds of children on the Internet. Given the levels of security we've seen from Indian governments, that sounds like a particularly bad idea.

Your neighborhoods are also getting CCTVs

Delhi has big plans for CCTVs in the works, and that's seriously worrying. But perhaps concerned about being left behind by the AAP in a race to the bottom, BJP MP Gautam Gambhir jumped the gun by installing CCTVs in his East Delhi constituency last month. At the time, Gambhir, who is currently in England for the Cricket World Cup, tweeted videos of the cameras being installed.

Although Delhi has a long history of using CCTV cameras, this latest installation wasn't done by any official body, but as a gift from a relatively unknown company, with no clarity on where the data from these cameras was going, who was watching the feeds, or where the records were being saved. Ultimately, Gambhir made an Instagram post on June 26, where he wrote that he was honoring the request of concerned citizens, and thanked one Deepak Bansal for taking the responsibility of the DVR.

However, a day before this, Hawkeye Systems, the company that was supposed to do the installation, told *The Indian Express* that it would not be going ahead with it because of the controversy. When Newslaundry asked the owner of Hawkeye about security measures for the cameras it

had already installed, he said he didn't know if there were any.

Real-time facial recognition systems are being built into CCTVs

On Friday, the National Crime Records Bureau (NCRB) put out a request for proposals for an automatic face recognition system. The last date for bids is August 16, but the NCRB is looking for a turnkey solution to build an Automatic Facial Recognition System (AFRS). The provider will have to supply, install and commission the hardware and software for this project. The detailed RFP states that this "is an effort in the direction of modernising the police force, information gathering, criminal identification, verification and its dissemination among various police organisations and units across the country".

The idea behind this is to build a national searchable database of faces, with an app that can be used on the field as well by officers who can snap a picture of a suspect, to compare against existing records gathered by the police. A similar system is already being used by different states, the biggest example being Punjab's PAIS project, whose developer Staqu also works with police in other states including Uttar Pradesh.

According to the RFP, the photographs used for the database to compare against pictures of suspect individuals will come from a number of different sources of information. Aside from police sources such as the CCTNS and ICJS databases, passports will also be used for this AFRS database. It is possible that the Aadhaar could also be used for this project—something a senior police officer hinted to *HuffPost India* in the past.

This new AFRS is meant to be integrated with existing systems, including the ones used by "advanced states". According to *MediaNama*, this includes the Delhi Police, which owns two facial recognition systems, and could also be integrated with the planned CCTV networks being deployed in the city. Other states such as Telangana, Gujarat, Tamil Nadu and

Karnataka are also being brought on board.

It's not clear what happens to the personal data of people gathered in this enterprise—whether it's only used for security or re-sold to businesses to 'properly monetise'—and in the absence of any proper data protection bill, there are no safeguards in place. And if that isn't enough, add to this questions about the effectiveness and reliability of such systems (famously, Amazon's Rekognition system misidentified pictures of American politicians as criminals).