TIF - The Digital Panopticon and How It Is Fuelled by Personal Data–II

ANURAG MEHRA

November 6, 2020

A 2007 mural by graffiti artist Banksy on Newman Street in London | Carolina Alves (CC BY-SA 2.0)

Personal data is being extracted and shared by private and state agencies; facial recognition is being used by governments to profile their citizens. What should we do and can we demand to resist this onslaught of surveillance that has been enabled by tech?

There is great potential for governments to use our data for coercive measures. Many governments, spurred by the availability of digital technologies that help acquire and store large amounts of data, have become quite zealous in collecting as much data as possible about citizens—detailed family histories, biometrics such as fingerprints, retinal scans and DNA profiles. The state-sponsored digital panopticon is now a reality. Authoritarian governments want to know 'everything' about you mostly for reasons of 'national security'. Ultimately, what they want to know is what your political inclinations are and therefore what kind of threat you pose to the ruling regime. Then, at an appropriate time they can target you with the right messages to garner support, to manipulate your ambivalence or to threaten you.

Of course, all the risks that apply to private data collections apply to this data as well: unauthorized access, breaches and hacks, processing of in ways that you never consented to, such as sharing with other

entities—including private contractors—and the interlinking of various databases maintained by the state.

In a stark instance of this, the Ministry of Road Transport and Highways in India, has developed a scheme to sell bulk, anonymized data pertaining to vehicle records, including financier, insurance and tax information.

The problems with facial recognition are many. Most images are obtained non-consensually or in coercive situations.

How much does the notion of consent apply to data 'taken' by the state, if a fundamental feature is to deny or curtail public services if you do not agree to 'give' your data? And how helpless will you be if your fingerprints and retinal scans are stolen to commit crimes in your name? To read more on this debate, surrounding India's Aadhar project, check out this interview with lawyer Usha Ramanathan and this very detailed report. The making of this ID is no longer optional because it has been linked to food supply through the public distribution system, banking, taxes, and every other possible public service.

The big risk: Facial recognition

One of the most significant threats to privacy in recent times comes from facial recognition technologies. The basic idea here is to capture images of faces, convert them into digitized data, and then search through existing databases to identify the person.

In the United States, big tech companies—IBM, Microsoft, Amazon—have decided not to offer this technology to the police, till its use is regulated by the legislation. Much of this has been inspired by the fear that it will aid racial profiling by state agencies, an aspect that has been driven home by the 'Black Lives Matter' protests. The European Union is contemplating a five-year ban to give time to policy makers to figure out how to react.

The problems with facial recognition are many. Most images are obtained non-consensually (e.g., in public spaces) or in coercive situations (e.g. airport arrival or departure); the technology still produces many mismatches especially with people of colour; and when fed into automated systems (immigration checkpoints, arrests, drone targets) biased algorithms engender racial/ethnic discrimination. This makes it a direct threat to civil liberties. An opinion piece in *Nature* pointed out, "These tools generate many of the same biases as human law-enforcement officers, but with the false patina of technical neutrality."

The first case of wrongful arrest, in the US, based on facial recognition was reported in June 2020 by the *New York Times*. A US university has carried out research that claims that facial recognition technology and AI can be used to "predict criminality", a proposition that has met with severe criticism. This idea has deep historical roots, and resurfaces every now and then.

Post-image capture, there are many 'innovative' ways in which image data can be processed. There is no better example of this than what is being done by ClearviewAI. This company scraped the internet, most significantly social media platforms, for facial images, and built a database containing billions of images. These are stored along with available personal identifiers plus the links where the images were scraped from. Any 'unknown' facial image uploaded into the ClearviewAI service is matched with the records that the company has to identify an individual. Also available are personal details as well as the links where this individual's images may be found. This service is simply astounding. It can be used by stalkers and was used by a billionaire to identify his daughter's boyfriend! Apparently, the police and other law enforcement agencies in the US have been using this service to identify people. Despite the company's claim that the service is not available to the public but only to law enforcement, its leaked list of clients has private companies, sports associations, and even immigration and customs departments in the US. Meanwhile, the company earlier this year suffered its first data breach.

There are no laws in India, and in most parts of the world, prohibiting, or even regulating, the use of facial recognition.

An even more frightening deployment, unused so far, is in augmented reality (AR) glasses. Imagine a police officer walking through a crowd of protesters; the AR glasses scan the faces of those who pass by and instantly flash on the glass, information about who this person is, where she stays, what websites host her photos, and what she does. Thus, dissenters and activists can be identified instantaneously. These are not imagined possibilities - the original NYT investigation of ClearviewAI reveals that the computer code already has the provision for pairing with such hardware built-in. Can it get more chilling than this?

Some senators in the US have proposed a law that imposes a nation-wide ban on facial recognition till federal regulations are in place. ClearviewAI has been sued in an Illinois court for collecting images of people "without any reason to suspect any of them of having done anything wrong, ever". Meanwhile, all tech majors— Google, YouTube, Facebook, Twitter, LinkedIn—have sent cease and desist notices to ClearviewAI to stop scraping data from their platforms,

And yet, despite all this public exposure about it, ClearviewAI is in negotiations with US state agencies to provide facial recognition services to track Covid patients.

Big Brother is watching (literally)

There are no laws in India, nor in most parts of the world, prohibiting, or even regulating, the use of facial recognition. Millions of images are captured everyday by publicly installed closed circuit TV (CCTV) cameras. The Delhi police has been using a software called Advanced Facial Recognition Software (AFRS) to surveil public gatherings to identify 'habitual' protestors. Now police in Vadodara are keen on using facial recognition technology offered by none other than ClearviewAI! A more detailed report describing the Indian scenario indicates the spread of facial recognition technology in policing to more areas in the country like Chennai, Hyderbad and Punjab. All of this is happening when the accuracy of the technology is only about 1-2%.

The home ministry has claimed that Delhi Police identified over 1,900 alleged rioters through facial scans obtained from CCTV footage, and recognized them using the driving license and voter-id databases (incidentally Delhi has one of the largest CCTV camera networks amongst cities, globally). Apparently, the Aadhar database was not used in this instance, though there have been demands to make this database accessible to the police. Many government agencies are excited about using facial recognition technology for various purposes, ranging from voter identification to airport passage, in railway stations, and now even schools.

With all forms of tracking enabled and working in tandem, the objective is to track every move a citizen makes.

The Chinese government has probably the largest databases of all varieties for its citizens. A recent, massive push is to acquire DNA data across the country. Some of the most surveilled cities are in China. All kinds of data acquisition happen through CCTVs, drones, biometric readers, and mobile apps. All persons applying for mobile phone connections have to undergo facial recognition verification. Payments made through QR codes are likely to be replaced by facial scans. Chinese banks have started to use 'micro-expression' analysis to check for signs of fraud by analysing facial movements, based on a technology developed by Ping An, a financial technology conglomerate.

A Financial Times report says, "Chinese facial recognition companies have taken the lead in serving this growing international market … because of the advantage they have … a massive domestic market and an authoritarian system where privacy often takes a back seat." With all forms of tracking enabled and working in tandem, the objective is to track every move a citizen makes.

Data-based ethnic profiling: The Uighurs

Nothing surpasses China's attempts in using facial recognition technology to control entire regions. Xinjiang province—where Muslim Uighurs live—is under heavy surveillance, like an open-air prison, flush with cameras as well as face scanners and biometric readers. Under the guise of health checks, all native individuals have been scanned for biometrics, DNA, blood type, voice recordings and face scans. Human Rights Watch shows us in this interactive website how the system monitors all the data collecting sensors—mobile phones locations, CCTV images, biometric scanners, to track the movement of individuals, and 'suspicious' behaviour can trigger alarms for the local police to act.

One of the most important objectives of advanced facial recognition software is the ability to recognize Uighur faces in real time. AI is being used on facial image databases so that the system becomes capable of identifying ethnicities and races from photos. A NYT report says that:

> … engineers feed data to artificial intelligence systems to train them to recognize patterns or traits. … they would provide thousands of labeled images of both Uighurs and non-Uighurs. That would help generate a function to distinguish the ethnic group.

An article on 'Terror Capitalism' poignantly cites a middle-aged Uighur businessman,

> The only kind of Uighur life that can be recognised by the state is the one that the computer sees. This makes Uighurs ... feel as though their lives only matter as data-code on a screen, numbers in camps. They have adapted their behaviour, and slowly even their thoughts, to the system.

Social credit systems

The Chinese can also lay claim to being pioneers in explicitly formulating the idea of a social credit system, analogous to the credit rating systems that banks use to assess the credit worthiness of borrowers. In the social credit system, individuals and even organizations are given scores that reflect how well they have been compliant with expected 'good' behaviour and how much in violation. Thus, behaviour—compliance with court judgements, paying fines in time—is tracked continuously at all times. Being on the 'blacklist' can lead to denial of train and plane tickets or access to a private school.

This system was supposed to have become completely operational in January 2020; but it now seems to have fallen into disarray as a complicated mixture of small, local projects. What is more unsettling is that many Chinese view it as a welcome step to increase compliance with lawful behaviour and the trustworthiness of people. As of March 2019, there were 13 million blacklisted people.

[W]e should demand that scraping and aggregation of public data be made illegal.

Yet, it has unleashed something with great devious potential, and it provides a window to what the world would look like if projects of this kind were weaponized by increasing scale and the use of AI. Now 'rating' is trickling into various sectors where the service provider rates the customer. Uber users have a score that is supposed to measure how nice they have been as customers. Uber has been 'banning' passengers with low ratings in some countries. Even Airbnb seems to have a guest rating system, though the extent to which it is used to deny bookings is not clear. Patronscan aggregates data about guests visiting restaurants, bars and clubs and then uses it to allow or deny entry to a guest. Much has appeared in the media questioning private ID scanning, including a detailed analysis. How long will it take before these 'social credit rating' systems proliferate like wildfire? As one commentator, Casey Newton, asks in her blog:

> As more companies acquire data sets about bad behavior among customers, the temptation to license that data to other companies could be irresistible. … won't the government seek access to that information as well? What will it do with that information, if so?

What we should demand

A guiding motto should be to minimize our data trails. As a broad charter we should insist on data laws that allow specific data extraction strictly for providing a given service, and not on vague promises of 'improving' services; end-user agreements that are short, crisp, free of legalese, and are comprehensible; clauses asking for consent to be prominently marked; rules that do not allow retention of data after the event (e.g. an Uber ride or a Google Map guided drive); mandatory controls for tuning of privacy, showing all the data collected, and enabling its deletion without much effort.

Further, we should demand that scraping and aggregation of public data be made illegal. For instance, no one should be able to collect all your public images; a ban on profiling, aggregation and sale of collected data to third parties; and, a moratorium on linking of databases, especially mixing of public and private ones.

> *Facial recognition has the potential for destroying privacy once and for all.*

Many of these core demands, or some variants thereof, are incorporated into the General Data Protection Regulation (GDPR, May 2018) of the European Union, as well as the California Consumer Protection Act (CCPA, January 2020) but that is just a start. There is still plenty of confusion in terms of the implications of these laws. The CCPA became operational in full force from July 2020.

Tech companies try their best to circumvent these new laws. This report by a Norwegian consumer group, aptly titled 'Deceived by Design', shows that for Facebook, Google and Windows 10,

> … default settings and dark patterns, techniques and features of interface design [are] meant to manipulate users, are used to nudge users towards privacy intrusive options. The findings include ... misleading wording, giving users an illusion of control, hiding away privacy-friendly choices, take-it-or-leave-it choices, and choice architectures where choosing the privacy friendly option requires more effort for the users.

And when they do 'comply' with the law—to reveal how much data they have about you—they show your data but with the vitals missing or in a form that you may not comprehend properly. A NYT report says that the detail

in which data is captured is “eye-popping”, like every tap of your kindle e-reader. No wonder that some policymakers argue that tech companies need to be broken up and given competition rather than just be regulated, as this makes their existing power ‘acceptable’. The most recent report prepared by a subcommittee of the US Congress notes how large tech companies wield monopoly powers, and the measures needed to tackle this.

The Personal Data Protection Bill, 2019 is pending in Parliament , amidst concerns that it gives unfettered freedom to state agencies to access anything.

Awareness of data extraction would also suggest that consumer devices and hardware should operate by default in ‘not-connected’ mode. The smartwatch may get your ECG but not send it to any server, only you should be able to send it to your doctor as and when you please. Devices should be able to do local, on-board processing of the inputs, whether it is digital assistants or sex toys. But, of course, this would take away almost all the motivation for selling such hardware where the main idea is to keep you ‘connected’ to the corporation’s data banks (perhaps for a fee)—and continue extracting data—rather than make a one off sale of a device.

Nationalism and ‘national security’ are being reinvented rapidly as the rationale for the deployment of an omnipresent state surveillance, driven by the unchecked acquisition of personal data.

The flurry of data extraction activity because of the novel coronavirus disease has led to a demand for data protection provisions in countries where they do not exist, like the US where there is no federal law yet on data privacy and security. In India, The Personal Data Protection Bill, 2019 is pending in Parliament, amidst concerns that it gives unfettered freedom to state agencies to access anything. The EU released a set of guidelines to overcome conflicts with the existing provisions in the GDPR in order to facilitate collection of data related to Covid-19. Legally and ethically, every regulation developed to fight the Covid disease, and the data collected under its provisions, should be reviewed critically. Except for health data of individuals, which should be secured in their confidential vaults, everything else, such as location and proximity data, and facial images, should be deleted when the pandemic ends.

Resistance

It is, of course, a cruel situation when the state turns upon its own citizens and ‘wants to know everything’ about them now that digital technologies have made this feasible. Nationalism and ‘national security’ are being reinvented rapidly as the rationale for the deployment of an omnipresent state surveillance, driven by the unchecked acquisition of personal data.

There are at least three interrelated consequences that arise: Firstly, state agencies are now equipped with efficient tools and sufficient data to find subversive individuals and ‘deal’ with them ‘appropriately’. If such individuals can be located, identified and tracked at all times there is very little that can save them from the depredations of a rogue state hell bent on preventing them from doing anything that is a threat to its rule.

Secondly, large databases containing diverse kinds of personal information and biometrics can be used to train algorithms, and automate the demonization of entire communities simply on the basis of how they look or even what they wear. A recent adverse ruling by a Dutch court on the use of algorithmic scores to identify people

'most likely to commit fraud' was based on the argument that the 'algorithm would begin associating poverty and immigrant status with fraud risk'. And, lastly, this creates an ethos of fear which conditions vast sections of the population to become submissive to authoritarian regimes and leaders.

> *[B]ehaviour prediction and modification is the new form of capitalism.*

While the state can use social credit to incentivize compliant behaviour in directions that it desires, private entities will use it to spawn unequal access to institutions and facilities. In an era that is seeing rapid privatization of public goods and services, such 'exclusivity' can be debilitating. Imagine if Uber is the only cab service provider available, but you cannot ride any because you have a low score. Such schemes are a horrible idea and must be opposed; we should demand that privacy laws should not permit collection of data that is the fuel for driving such a system.

It is appropriate to close with a quote from one of the most incisive books written about capitalism configured for the digital era. Shoshana Zuboff argues in her book 'The Age of Surveillance Capitalism' that behaviour prediction and modification is the new form of capitalism:

> Surveillance capitalism unilaterally claims human experience as free raw material for translation into behavioural data. Although some of these data are applied to service improvement, the rest are declared as a proprietary behavioural surplus, fed into advanced manufacturing processes known as 'machine intelligence', and fabricated into prediction products that anticipate what you will do now, soon, and later.

These products are then used to manipulate or threaten us.

This is the second and concluding article in a two-part series. Read the first part here.

The India Forum *welcomes your comments on this article for the Forum/Letters section.*
Write to editor@theindiaforum.in.

Tags: Technology
Surveillance
Privacy
Government
Data