

# **Procurement of Facial Recognition Technology for Law Enforcement in India: Legal and Social Implications of the Private Sector's Involvement**

**Working Paper 3 | December 2021**

**V | D | H |** Centre for  
Legal Policy

Better laws | better governance

**This working paper is an independent, non-commissioned piece of research undertaken by the Vidhi Centre for Legal Policy, an independent think tank doing legal research to help make better laws.**

# About the Authors

---

Ameen Jauhar is a Senior Resident Fellow at the Vidhi Centre for Legal Policy, leading its Centre for Applied Law & Technology Research. Ameen's focus areas include AI ethics and governance, and the use of AI in legal and justice systems.

Jai Vipra is a Senior Resident Fellow at the Centre for Applied Law & Technology Research. Her focus areas include the digital economy, data commons, algorithmic regulation, digital trade and fintech.

The authors would like to thank Smriti Parsheera for her detailed and invaluable inputs which have led to this iteration of the working paper.

# About the Centre for Applied Law & Technology Research

---

The Centre for Applied Law and Technology Research (ALTR) has been established within Vidhi to spearhead original, independent research on crucial issues emerging within the law and technology domain. The team was formally constituted in September 2020, comprising an interdisciplinary roster of researchers from both legal and social science backgrounds. The Centre's key objective is to conduct high quality research, as well as engaging with the main stakeholders to translate our academic work into actionable reforms. Our ongoing work focuses on three main areas: internet and data governance; digital economy; and AI ethics and governance of AI. In pursuit of its research and policy work, ALTR has forged crucial partnerships and collaborations, including those with the UN Resident Coordinator's office, IIIT Delhi, NITI Aayog, Dept. of Transport (Govt. of NCT of Delhi), etc., among other stakeholders.

# Table of Contents

About the Authors.....	2
About the Centre for Applied Law & Technology Research.....	3
Introduction.....	2
Methodological issues.....	5
I. Private sector technology provision and law enforcement.....	7
II. Issues caused by private sector involvement in FRT for law enforcement.....	12
Privacy risks.....	12
Issues surrounding unclear legal liability.....	15
Private goals drive public priorities.....	16
III. Recommendations.....	20
Transparency of agreements.....	20
Algorithmic standards and regulation.....	20
Stricter legal restrictions on surveillance.....	21
Public involvement in decision-making.....	21
Conclusion.....	23
Annexure - 1.....	24
Annexure - 2.....	25
Annexure - 3.....	26

# Introduction

---

Artificial intelligence (AI) technologies have seen a rapid uptake in government applications, and across sectors. For India, arguably a major and contentious use of AI is the ubiquitous deployment of facial recognition tech (FRT), especially by local law enforcement agencies.<sup>1</sup> Given the paucity of independent scholarship, especially from an Indian context, on these issues, we decided to examine some unique aspects to this debate, through doctrinal and empirical methods of research. This working paper is the final one in our three part series examining different aspects of how FRT is featured in Indian law enforcement. The first working paper presented a deep dive into the legal and constitutional challenges, and ethical and design risks in the use of this technology in the criminal justice system (specifically policing and surveillance).<sup>2</sup> The second working paper was an empirical study of the impact such technology is likely to have on already vulnerable populations, through a case study of its use by the Delhi Police.<sup>3</sup>

AI in law enforcement has multiple uses. Basu and Hickok (2018) have compiled the range of such applications in India and show that these primarily fall under the categories of predictive analytics, and speech or facial recognition.<sup>4</sup> For instance, Delhi Police's Crime Mapping, Analytics and Predictive System (CMAPS) is an example of the deployment of predictive analytics for law enforcement.<sup>5</sup>

FRT, which is a form of AI application, has found an increasing use in Indian law enforcement. Several states have at least one form of FRT system, most commonly one that links with a network of CCTV cameras and is used for local policing. In utility, it ranges diversely from finding missing children, keeping an eye on busy marketplaces, profiling protestors and also ostensibly "protecting women".<sup>6</sup> The most overt intent of deploying FRT for law enforcement purposes came in 2018. The National Crime Records

---

<sup>1</sup>Ameen Jauhar. Facing up to the Risks of Automated Facial-Recognition Technologies in Indian Law Enforcement. *Indian Journal of Law and Technology*, 16(1). 2020.

<sup>2</sup> Ameen Jauhar. Indian Law Enforcement's Ongoing Usage of Automated Facial Recognition Technology – Ethical Risks and Legal Challenges. Vidhi Centre for Legal Policy. 2021. Available at: <https://vidhilegalpolicy.in/research/indian-law-enforcements-ongoing-usage-of-automated-facial-recognition-technology-ethical-risks-and-legal-challenges/>

<sup>3</sup> Jai Vipra. The Use of Facial Recognition Technology for Policing in Delhi. Vidhi Centre for Legal Policy. 2021. Available at: <https://vidhilegalpolicy.in/research/the-use-of-facial-recognition-technology-for-policing-in-delhi/>

<sup>4</sup> Arindrajit Basu and Elonnai Hickok. Artificial Intelligence in the Governance Sector in India. The Centre for Internet and Society. 2018. Available at: <https://cis-india.org/internet-governance/ai-and-governance-case-study-pdf>

<sup>5</sup> Vidushi Marda and Shivangi Narayan. Data in New Delhi's Predictive Policing System. FAT '20: Proceedings of ACM Conference on Fairness, Accountability, and Transparency. January 27–30, 2020. Available at: <https://www.vidushimarda.com/storage/app/media/uploaded-files/fat2020-final586.pdf>

Bureau (NCRB) floated a request for proposal (RFP) for the provision of a pan-Indian FRT system for law enforcement.<sup>7</sup> After considerable concerns were voiced against it, including a legal notice being served,<sup>8</sup> the tender was modified such that the technology would not be linked to multiple databases.<sup>9</sup>

The proliferation of FRT in the domain of law enforcement is concerning on various fronts which has been the subject of detailed discussion in the first working paper of this series. Briefly, it poses an obvious risk to privacy, as people are put through surveillance and analytical systems tracking their everyday activities. In the absence of a data protection law, there is very little if any protection against privacy harms caused by the use of this technology. Surveillance with the use of FRT can also lead to small crimes or infractions being punished disproportionately as these become easier to track. The use of FRT can lead to significant bias against marginalised people, especially those who already face a bias from the police. We have covered these risks in detail in the previous two papers in this series.<sup>10</sup>

However, a crucial aspect of the whole debate around the use of FRTs in law enforcement, both internationally and here in India, that is conspicuously absent is how the private sector works in tandem with local and federal governments, and law enforcement agencies to design these surveillance systems. Arguably, *prima facie*, this is emblematic of either the lack of publicly accessible data on such private public contracts, or exhibits a lack of real consideration of its innate risks and challenges. Whatever the reason, at present, state governments across India have continued to procure such technologies while circumventing any public scrutiny and accountability. Therefore, as the concluding working paper in our series, here we will focus on the involvement of the private sector in developing and implementing FRT solutions for law enforcement in India.

The paper is structured in the following sections. First, we discuss the methodological issues we faced while conducting our empirical research on the private sector's participation in this area in India. Our difficulties themselves are symptomatic of the

---

<sup>6</sup> Aihik Sur. Lucknow Safe City Project: Uttar Pradesh To Deploy Facial Recognition, 'Label' Faces Of Suspects. Medianama. August 19, 2021.

<sup>7</sup> National Crime Records Bureau (NCRB). Request For Proposal To procure National Automated Facial Recognition System (AFRS). 28 June 2019.

<sup>8</sup> Internet Freedom Foundation. IFF's Legal Notice to the NCRB on the Revised RFP for the National Automated Facial Recognition System #ProjectPanoptic. 15 July 2020. Available at: <https://internetfreedom.in/iffs-legal-notice-to-the-ncrb-on-the-revised-rfp-for-the-national-automated-facial-recognition-system/>

<sup>9</sup> National Crime Records Bureau (NCRB). Request For Proposal To procure National Automated Facial Recognition. 22 June 2020.

<sup>10</sup> Ameen Jauhar. Indian Law Enforcement's Ongoing Usage of Automated Facial Recognition Technology – Ethical Risks and Legal Challenges. Vidhi Centre for Legal Policy. 2021 and Jai Vipra. The Use of Facial Recognition Technology for Policing in Delhi. Vidhi Centre for Legal Policy. 2021.

opacity surrounding these contracts. Following the methodology enunciation, chapter I provides an overview of the contribution of the private sector to facial recognition systems in law enforcement worldwide; chapter II does the same for India. Chapter III outlines the unique issues raised because of the involvement of the private sector in this field, and chapter IV makes policy recommendations based on the research so far presented.



# Methodological issues

---

We encountered media reports naming private companies and describing their involvement in providing FRT to police agencies in different states. Coupled with our desk review of existing literature on the subject, we encountered a gap on how private corporations are being onboarded by governments for designing and deploying FRT systems for local police forces.

Like us, other researchers and activists in India have tried to file Right to Information (RTI) applications with various government agencies to understand their use of FRT.<sup>11</sup> Commonly, among other things, these applications have inquired about the involvement of the private sector in providing FRT to different agencies (including law enforcement ones). The National Highways Authority of India, when questioned about its use of FRT, stated that the tender was under process.<sup>12</sup> RTI applications filed with the Delhi Police were denied information under Section 8(1)a of the Right to Information Act, which provides an exception if the given information could violate trade secrets or intellectual property.<sup>13</sup>

In a similar vein and in order to make our work data driven, we filed several rounds of RTI applications with different state police headquarters, and even state governments. Specifically, we filed these applications with the police forces in the cities of Surat, Hyderabad and Chennai, and the state of Punjab. These latter four identified media reportage of local police forces claiming private sector participation, or our own research (limitedly available as it was) on private entity(ies) claiming to have worked with these forces.<sup>14</sup> A template of the RTI application filed, is annexed as **Annexure 1**. Furthermore, where a police HQ or a state government responded, it was in denial of such an engagement with the private sector. For example, the Public Information Officer for the Police Commissioner of Surat stated in their response that there was no agreement between the concerned private company and itself. This would mean that the reported use of FRT provided by the Japanese company NEC to Surat was carried out without a

---

<sup>11</sup>See for instance Internet Freedom Foundation's Project Panoptic: <https://internetfreedom.in/tag/project-panoptic/>

<sup>12</sup> The RTI response can be found here: <https://drive.google.com/file/d/1yyVGMBR6nhsZ6cw5qlrCFtj4dJ5CqeTh/view>

<sup>13</sup> Internet Freedom Foundation. Project Panoptic: Right to Information Updates from Delhi Police, Kolkata Police and Telangana State Technology Services. Available at: <https://internetfreedom.in/project-panoptic-right-to-information-updates/>

<sup>14</sup> Anand Murali. The Big Eye: The tech is all ready for mass surveillance in India. Factor Daily. August 13, 2018. Available at: <https://archive.factoraily.com/face-recognition-mass-surveillance-in-india/>

contract, or that the news report was false.<sup>15</sup> However, details of the technology provision can be found on NEC’s website as well, with a quote from the Police Commissioner of Surat City.<sup>16</sup> The RTI reply is annexed to the paper as **Annexure 2**. Given the evasive content of responses received, and factoring in the time and resource constraints of the authors, we did not appeal these decisions. Thus, we were greatly limited by the opacity of police departments with respect to the use of these technologies, and have gone on to identify them as one of the main challenges in the use of FRT by local law enforcement in India.<sup>17</sup>

Below is a table giving an overview of the RTIs we filed for this paper and the responses we received:

<b>Date of filing</b>	<b>Agency</b>	<b>Private sector entity</b>	<b>Response received</b>	<b>Details</b>
08/07/2021	Inspector General of Police, Tamil Nadu	FaceTagr	No	The application was forwarded to the Public Information Officer, T. Nagar; no response was received after this.
08/07/2021	Director General of Police, Punjab	Staqu	No	The application was forwarded to the Asst. Information General (Police/Provisioning) and AIG (Police/HQ, Intelligence). No response was received after this.
08/07/2021	Police Commissioner of Surat	NEC	Yes	The Public Information Officer denied that any agreement had been signed with NEC as per the information requested.
07/09/2021	Director General of Police, Telangana	Unknown	No	-

In view of our repeated dead-ends through the RTI route, as an alternative, we conducted some unstructured interviews and discussions with researchers and academics who are

<sup>15</sup> Yagnesh Bharat Mehta. In a first, real-time facial recognition system launched by Surat Police. *The Times of India*. July 19, 2015. Available at: <https://timesofindia.indiatimes.com/city/surat/in-a-first-real-time-facial-recognition-system-launched-by-surat-police/articleshow/48135306.cms>

<sup>16</sup> NEC provides Face Recognition Technology to Surat City Police. February 25, 2015. Available at: [https://www.nec.com/en/press/201502/global\\_20150225\\_03.html](https://www.nec.com/en/press/201502/global_20150225_03.html)

<sup>17</sup>

also working in this space, or related issues. The objective here was to determine if the opacity we faced was the norm, or an exception we encountered in our work. We also want to caveat this by stating that the role of the private sector and how it has partnered with the governments in India for deploying surveillance technology, specifically FRT, is rather under examined. Hence, our conversations were not extensive, and had to be supplemented with our own insights of researching this issue through extensive literature reviews of both Indian and foreign scholarship.

# I. Private sector technology provision and law enforcement: an overview

---

In January 2020, the New York Times broke a story about an American company called Clearview AI.<sup>18</sup> Clearview AI scrapes data from social media and other publicly available sources anywhere on the Internet, to create a powerful facial recognition tool. This FRT, among other entities, was licensed to domestic law enforcement agencies in the US and several other countries.<sup>19</sup> Police personnel can click a picture of a person and understand a large part of their digital footprint through their faces using the app.<sup>20</sup> The company provides its technology to at least 600 police agencies in the United States, and at least 2,000 American public agencies in total.<sup>21</sup> In May 2021, privacy activists filed legal challenges in different European countries against Clearview AI.<sup>22</sup> Despite its scale, Clearview AI is only one of the companies providing FRT to law enforcement agencies in the United States.

Over the last few years, employees of large technology companies along with civil society activists have forced these companies to desist from providing FRT to governments for surveillance functions. Amazon and Microsoft have both announced moratoria on providing FRT to the police, while IBM has ended its general facial recognition programme altogether.<sup>23</sup> Most recently, the now rebranded Facebook (as Meta) announced discontinuation of its facial recognition programme.<sup>24</sup> However, it is pertinent to mention that these self-regulatory measures come belatedly. For instance, before it was forced to end these partnerships, Amazon's subsidiary Ring had made deals with 1,300 law

---

<sup>18</sup> Kashmir Hill. *The Secretive Company That Might End Privacy as We Know It*. The New York Times. January 18, 2020. Available at: <https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html>

<sup>19</sup> Ibid.

<sup>20</sup> Ibid.

<sup>21</sup> Robert Hart. *Clearview AI — The Facial Recognition Company Embraced By U.S. Law Enforcement — Just Got Hit With A Barrage Of Privacy Complaints In Europe*. Forbes. May 27, 2021. Available at: <https://www.forbes.com/sites/roberthart/2021/05/27/clearview-ai---the-facial-recognition-company-embraced-by-us-law-enforcement---just-got-hit-with-a-barrage-of-privacy-complaints-in-europe/?sh=190211317f53>

<sup>22</sup> Ibid.

<sup>23</sup> Rebecca Heilweil. *Big tech companies back away from selling facial recognition to police. That's progress*. Vox. June 11, 2020. Available at: <https://www.vox.com/decode/2020/6/10/21287194/amazon-microsoft-ibm-facial-recognition-moratorium-police>

<sup>24</sup> Jerome Pesenti. *An Update On Our Use of Face Recognition*. Facebook. November 2, 2021. Available at: <https://about.fb.com/news/2021/11/update-on-use-of-face-recognition/>

enforcement agencies to use CCTV camera footage for surveillance.<sup>25</sup> Similarly, before Microsoft was forced to enact its moratorium, it had pitched its FRT system to the Drug Enforcement Administration, which has often come under heavy criticism for its racist and brutal policies.<sup>26</sup> Microsoft and Amazon have not extended their moratoria to cover federal law enforcement agencies in the US.<sup>27</sup> Aside from this loophole, there are several other large and small private companies that still provide FRT to the police.<sup>28</sup>

In 2012, IBM entered into an agreement with the government of Davao in the Philippines to provide a surveillance system for the city.<sup>29</sup> The system, provided by IBM till 2016, reportedly assisted in the extrajudicial killings carried out by President Rodrigo Duterte in his “war on drugs”.<sup>30</sup> While IBM denies that the system included FRT, promotional material reveals that IBM advertised FRT as being part of the system.<sup>31</sup> The system also enabled the over-criminalisation of petty crime like loitering.<sup>32</sup>

FRT does not have to be directly provided to the police for it to be used for law enforcement functions. At times there is monitoring by non-state actors that also indirectly feeds into arbitrary surveillance. For instance, real estate companies use FRT in many parts of the world to restrict entry to, or detect crime in, their premises. In China such use has been particularly prevalent - both for security and advertising purposes.<sup>33</sup> A survey revealed that over eighty percent of people in China wanted more control over their data collected by such systems.<sup>34</sup> Subsequently, several provinces and cities in China have banned or are considering banning the use of FRT for security purposes.<sup>35</sup> China also released draft standards for the use of FRT, limiting its use to identification rather than prediction, discouraging its use on minors, and recommending a search for alternatives to the technology before implementation.<sup>36</sup> There are also examples of real estate

---

<sup>25</sup> Karen Hao. The two-year fight to stop Amazon from selling face recognition to the police. MIT Technology Review. June 12, 2020. Available at: <https://www.technologyreview.com/2020/06/12/1003482/amazon-stopped-selling-police-face-recognition-fight/>

<sup>26</sup> Zack Whittaker. Microsoft pitched its facial recognition tech to the DEA, new emails show. TechCrunch. June 17, 2020. Available at: <https://techcrunch.com/2020/06/17/microsoft-dea-facial-recognition/>

<sup>27</sup> Ibid.

<sup>28</sup> Cathy O’Neill. Opinion: Big Tech Can’t Stop Facial Recognition by Itself. Government Technology. June 17, 2020. Available at: <https://www.govtech.com/opinion/opinion-big-tech-cant-stop-facial-recognition-by-itself.html>

<sup>29</sup> George Joseph. Inside The Video Surveillance Program Ibm Built For Philippine Strongman Rodrigo Duterte. The Intercept. March 20, 2019. Available at: <https://theintercept.com/2019/03/20/rodrigo-duterte-ibm-surveillance/>

<sup>30</sup> Ibid.

<sup>31</sup> Ibid.

<sup>32</sup> Ibid.

<sup>33</sup> Phoebe Zhang. Privacy in China: the growth of facial recognition technology in the private sector raises concerns about security and identity. South China Morning Post. Available at: <https://www.scmp.com/lifestyle/article/3111428/privacy-china-growth-facial-recognition-technology-private-sector-raises>

<sup>34</sup> Ibid.

<sup>35</sup> Ibid.

companies in Canada<sup>37</sup> and the United States<sup>38</sup> using FRT to screen residents and visitors. In Brazil, public schools use FRT to track attendance and ostensibly assure safety.<sup>39</sup> Much of Brazil's surveillance equipment is provided by Huawei and operated by the private telecom company Oi Soluções.<sup>40</sup>

In a resolution, the European Parliament has called for a ban on both facial recognition technology and predictive policing.<sup>41</sup> It also called for a ban on private facial recognition databases. However, this resolution is non-binding.<sup>42</sup>

In India, it is primarily news reports that provide information on the involvement of private companies in providing FRT to the police. There is no data or documented records made available to the public by the law enforcement agencies involved, and as revealed by our RTI endeavours, the application is opaque.

News reports reveal that a few Indian startups such as Staqu<sup>43</sup>, Innefu Labs<sup>44</sup> and FaceTagr<sup>45</sup> provide FRT to the police. Foreign companies like Japan's NEC and Israel's Cortica are also providers of FRT to the police. Other private companies such as EY, Idemia<sup>46</sup>, Tech5<sup>47</sup>, Thales<sup>48</sup>, Anyvision<sup>49</sup> and Vara Technology<sup>50</sup> have been present at pre-bid conferences organised by the National Crime Records Bureau (NCRB) for developing a national facial recognition system.<sup>51</sup>

---

<sup>36</sup> Hunton Andrews Kurth. China Publishes Draft Security Standard on Facial Recognition. April 29, 2021.

Available at: <https://www.huntonprivacyblog.com/2021/04/29/china-publishes-draft-security-standard-on-facial-recognition/>

<sup>37</sup> Chris Arsenault. Forgot your keys? Scan your face, says Canadian firm amid privacy concerns. Reuters. April 6, 2020. Available at: <https://www.reuters.com/article/us-canada-tech-homes-feature-trfn/forgot-your-keys-scan-your-face-says-canadian-firm-amid-privacy-concerns-idUSKBN21O1ZT>

<sup>38</sup> Condos in South Beach add facial recognition to robust security platform. Security Magazine. Available at: <https://www.securitymagazine.com/articles/94061-condos-in-south-beach-add-facial-recognition-to-robust-security-platform>

<sup>39</sup> Charlotte Peet. Brazil's embrace of facial recognition worries Black communities. Rest of World. Available at: <https://restofworld.org/2021/brazil-facial-recognition-surveillance-black-communities/>

<sup>40</sup> Ibid.

<sup>41</sup> Melissa Heikkila. European Parliament calls for a ban on facial recognition. Politico. Available at: <https://www.politico.eu/article/european-parliament-ban-facial-recognition-brussels/>

<sup>42</sup> Ibid.

<sup>43</sup> <https://www.staqu.com/>

<sup>44</sup> <https://www.innefu.com/>

<sup>45</sup> <https://facetagr.com/>

<sup>46</sup> <https://www.idemia.com/>

<sup>47</sup> <https://tech5.ai/>

<sup>48</sup> <https://www.thalesgroup.com/en>

<sup>49</sup> <https://anyvision.co/>

<sup>50</sup> <https://varatechnology.com/>

<sup>51</sup> Soumyarendra Barik. Exclusive: Concerns Around Number Of Active Users, And 'Backdoors' Raised At An NCRB Facial Recognition Meeting. Medianama. July 13, 2020. Available at: <https://www.medianama.com/2020/07/223-automated-facial-recognition-system-india-bidders-concern/>

We have been able to glean the following types of uses of FRT by the police in India:

1. **Real time monitoring of public places:** Police use FRT to monitor public places to identify “blacklisted” people among the crowd. Staqu, for instance, has stated that its FRT can identify people based on a low resolution video feed as well.<sup>52</sup>
2. **Investigation:** Police also use FRT for narrowing a list of suspects, tracking down suspects and potentially using this information as evidence during trial. For example, the Bihar police floated a tender in April 2021 requesting an integrated surveillance system that could, among other capabilities, match faces of suspects to various databases.<sup>53</sup> In a case involving sandalwood smuggling, the Karnataka police claimed that a month-long investigation could have been completed in a week had they been able to use FRT.<sup>54</sup>
3. **Smartphone-based instant search and verification:** FaceTagr claims that it has helped Chennai police use an app which can match a person’s face to a database instantly, through the use of a picture clicked on the spot.<sup>55</sup> In 2017, it was reported that the database included 12,000 offenders, to be increased to an additional 40,000.<sup>56</sup> Police collected the initial database themselves.<sup>57</sup>
4. **Conflict area monitoring:** FRT is also reportedly being used by the Indian armed forces.<sup>58</sup> Staqu reportedly conducts aerial imaging analysis for the Indian Army.<sup>59</sup> Army documents show that there is a requirement for AI-based field monitoring with the use of legacy cameras such that resources are freed up from the time-consuming task of monitoring camera feeds.<sup>60</sup> They also show that as of 2019 there was no real time FRT deployed by the Indian Army.<sup>61</sup> The Indian Army has

---

<sup>52</sup> Jarvis. Available at: <https://www.staqu.com/jarvis/>

<sup>53</sup> Aihik Sur. Bihar Looking To Deploy Facial Recognition System In Bhagalpur And Muzaffarpur, Connect It To CCTNS. Medianama. April 19, 2021. Available at: <https://www.medianama.com/2021/04/223-bihar-bhagalpur-muzaffarpur-facial-recognition-cctns/>

<sup>54</sup> Rajiv Kalkod. 23 lakh portraits enter facial recognition database of Karnataka police. The Times of India. September 25, 2021. Available at: <https://timesofindia.indiatimes.com/city/bengaluru/23-lakh-portraits-enter-facial-recognition-database-of-karnataka-police/articleshow/86506266.cms>

<sup>55</sup> FaceTagr Home Page: <https://facetagr.com/>

<sup>56</sup> A Selvaraj. Cops use mobile app to scan faces, crack cases. The Times of India. November 16, 2017. Available at: <https://timesofindia.indiatimes.com/city/chennai/cops-use-mobile-app-to-scan-faces-crack-cases/articleshow/61665626.cms>

<sup>57</sup> Ibid.

<sup>58</sup> Radhika Udas. Meet These 5 Indian AI Startups That Are Making The World A Better Place. Express Computer. February 17, 2020. Available at: <https://www.expresscomputer.in/artificial-intelligence-ai/meet-these-5-indian-ai-startups-that-are-making-the-world-a-better-place/49184/>

<sup>59</sup> Sanchita Dash. EXCLUSIVE: This Indian startup has made a profit solving 1,100 police cases with just one round of funding. Business Insider. June 20, 2019. Available at: <https://www.businessinsider.in/staqu-turns-profitable-after-1100-police-cases-and-one-funding-round/articleshow/69871636.cms>

<sup>60</sup> Army Design Bureau. Compendium – Problem Definition Statements (Volume IV), pp. 3. 2019. Available at: <https://indianarmy.nic.in/makeinindia/CPDS%20Vol%20IV%202019.pdf>

<sup>61</sup> Ibid, pp. 15

published problem statements in order to encourage research and development by both public and private actors in these technologies.<sup>62</sup>

5. **Covid-related monitoring:** FRT was used for verifying beneficiaries at vaccination centres as part of Covid-19 prevention measures in India. Since vaccination was age-restricted and tracking the number of shots per person is important, identity verification fulfilled a law enforcement purpose. FRT was used to match people's photos at the vaccination site with the Aadhaar photos, although the details of this use are scant.<sup>63</sup>

This list is not exhaustive, as there can exist uses of FRT that are not revealed in the public domain. However, it is indicative of the broad contours of usage by law enforcement agencies in India and how the private sector designs these for them.

The data on standards followed by or required from private providers of FRT for law enforcement is also scant. In its revised tender for a national facial recognition system, the NCRB required bidders to have participated in an NIST evaluation.<sup>64</sup> NIST is the National Institute of Software and Technology (of the US), and conducts a facial recognition vendor test that assesses FRT on accuracy and demographic bias. To our knowledge, information about FRT accuracy standards requirements during the tender process is not public (for law enforcement applications). It is also pertinent to mention there is an argument to be made on the efficacy of an American test for an FRT tool to be designed and deployed in India, using Indian datasets.

The following section elaborates on the list of problems caused or likely to be caused by the use of privately provided FRT by law enforcement.

---

<sup>62</sup> Ibid.

<sup>63</sup> Scroll Staff. Covid: Facial recognition is being used to verify vaccine beneficiaries, says Centre in RTI reply. Scroll.in. July 6, 2021. Available at: <https://scroll.in/latest/999443/covid-facial-recognition-is-being-used-to-verify-vaccine-beneficiaries-says-centre-in-rti-reply>

<sup>64</sup> Soumyarendra Barik. NCRB Drops CCTV Integration Clause From Updated Facial Recognition Tender, Eases Bid Qualification Criteria For Vendors. Medianama. July 2, 2020. Available at: <https://www.medianama.com/2020/07/223-afrs-revised-tender-ncrb/>



## II. Issues caused by private sector involvement in FRT for law enforcement

---

There are both legal and governance questions raised due to the involvement of the private sector in providing FRT for law enforcement. Some questions are related to privacy, particularly in the indiscriminate use of various datasets, the outsourcing of surveillance functions to private entities, and the security of data used in FRT processes. Some questions are related to the thorny issues of liability that arise in the use of AI applications. Other questions relate to the blending of private incentives with public power in security operations. This section elaborates on all of these issues.

### Privacy risks

There are serious concerns in terms of informational autonomy and privacy of individuals. FRT uses sensitive and unique information and facial prints which are akin to biometrics, and certainly classify as personal data or information as laid down by the Supreme Court of India in the *Puttaswamy* judgment.<sup>65</sup> While India awaits a formal data protection legislation to be enacted, it is incorrect to assume that private and public entities have a *carte blanche* on how to collect, process and utilise personal data of individual citizens. At the same time, the concept of informational autonomy has been recognised and found to be a key manifestation of the *right to privacy* under Article 21 of the Constitution.

This has significant implications with the current form of surreptitiously engaging private corporations to design, deploy, and oversee the use of FRT in Indian law enforcement. The most significant issue is what datasets are being used by these companies to design the underlying FRT algorithms. For instance, when the NCRB's original request for proposal to set up a pan-Indian FRT system, gave a loosely worded description of the datasets that may be used, it immediately drew a sharp response from lawyers and privacy activists.<sup>66</sup> Following the issuance of a legal notice, it compelled the NCRB to recast the usable

---

<sup>65</sup> K. S. Puttaswamy v. Union of India (2017) 10 SCC 1

<sup>66</sup> This has also been argued in a legal notice served to the NCRB seeking rescinding of its request for proposals for the nationwide AFRS. ISee Internet Freedom Foundation. Rejoinder to Reply dated November 5, 2019. Available at: <https://drive.google.com/file/d/1Cb9BtyS17Z7IM7tvAJGNRqQ96ypAGtbN/view>

datasets in a much more clearly defined manner in its revised RFP.<sup>67</sup> For most states, where companies have designed such algorithms, it is completely unclear as to whether sensitive, personal data of Indians is being tapped into without their informed consent, in violation of the right to privacy, or not. This also conflicts with the notion that an individual must have control over what personal information is collected, used, or shared further, as established by the Supreme Court in *Puttaswamy*.<sup>68</sup> On the other hand, if datasets comprising Indian faces are not being used in the training of the algorithm, there are other risks like inherent design flaws leading to inaccurate outcomes. We have covered these in detail in our first working paper of the series.<sup>69</sup>

Beyond the question of datasets, there is a significant concern of whether surveillance activities are directly or indirectly being outsourced to these private corporations. Surveillance, even when conducted by the state, is exceptional and governed by laws. Without commenting on the merit or demerit of state surveillance, it is unquestionable that private entities are not empowered to assume this role, nor is this a responsibility the state may freely delegate. The opacity which shrouds the current engagements of state police forces or governments in India with limited private entities, their roles and scope of engagement, and the access they arguably can continue to have over the underlying algorithm, warrants serious questions on the plausible and dangerous merger of state functions with a private entity. This has virulent ramifications from a democratic, as well as privacy standpoint, the latter being the power of mass surveillance being afforded to shadowy private sector entities.

The third issue in infraction to an individual's right to privacy is the potential breach of data that private entities designing such algorithms, may precipitate. The draft Personal Data Protection Bill, 2019 (PDP Bill) has proposed considerable onus on data processors by prescribing stringent measures in terms of data collection, storage, access controls, etc.<sup>70</sup> However, in the absence of this formal legislation, and again, due to the lack of public visibility or any scrutiny of how the private sector entities are operating in this space of designing surveillance systems, there is a legitimate concern on where datasets being used are safeguarded with appropriate mechanisms in place. In fact, in India, there

---

<sup>67</sup> National Crime Records Bureau (NCRB). Request For Proposal To procure National Automated Facial Recognition. 22 June 2020.

<sup>68</sup> See *Puttaswamy* supra n.65; Vrinda Bhandari, et al. *An Analysis of Puttaswamy: The Supreme Court's Privacy Verdict*. *IndraStra Global*, 11, 1-5. 2017. Available at <https://nbn-resolving.org/urn:nbn:de:0168-ssoar-54766-2>; see also Abhishek Gupta et. al. *The Privacy Conundrum: An empirical examination of barriers to privacy among Indian social media users*. In Sudhir Krishnaswamy and Divij Joshi (eds), *The Philosophy and Law of Information Regulation in India*. CLPR. 2021 (Forthcoming).

<sup>69</sup> Ameen Jauhar. *Indian Law Enforcement's Ongoing Usage of Automated Facial Recognition Technology – Ethical Risks and Legal Challenges*. Vidhi Centre for Legal Policy. 2021.

<sup>70</sup> *The Personal Data Protection Bill, 2019*. Bill No. 373 of 2019. As Introduced in Lok Sabha. Available at: [http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373\\_2019\\_LS\\_Eng.pdf](http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf)

have been reported instances of data leaks from FRT applications being used by local police agencies.<sup>71</sup> Data breaches can both be accidental and deliberate.

The example of Clearview AI might help to illustrate this point further. As Clearview AI is used by so many police departments in the United States, it now has a database of all the people that the police search for.<sup>72</sup> This is a database that can be looked at in many different ways depending on one's understanding of police work: it can be seen as a list of vulnerable people, criminals, or people given to crime. What happens when a database of such people is used for other purposes? Let us assume the police runs searches on the face of a person for being a suspect, but later decides he is not a suspect. It is obviously and evidently inappropriate for this search information to land up with a credit rating agency, a housing society, child adoption centres, and employers. The risk of unfair discrimination is clear and intense. The search data does not even have to be tied to a certain name for it to be used maliciously - aggregate data always carries a risk of de-anonymisation, and entities like credit rating agencies use locality-based data to rate entire neighbourhoods as well.<sup>73</sup>

In India, the national-level facial recognition system to be developed for the NCRB would connect to the Crime and Criminal Tracking Network and Systems (CCTNS) database. The private FRT vendor would have access to this database in some form, or at the very least will have access to inferences made from this database. There is no clear manner in which the private vendor will be prevented from using this database jointly with FRT data for unrelated purposes, such as by selling it to a credit rating agency by bypassing legal restrictions against such sharing.<sup>74</sup>

As another example, Staqu has now started providing its software for private security uses such as those in real estate.<sup>75</sup> There is no transparency on what kind of data is used to aid private security providers to meet their ends, and Indian law is woefully inadequate at limiting such practices.

---

<sup>71</sup> Gopal Sathe. This Crime Fighting App Is Leaking Criminals', Citizens and Even Police's Info. HuffPost India. June 9, 2019. Available at: [https://www.huffpost.com/archive/in/entry/copseye-facial-recognition-data-leak\\_in\\_5d7255a4e4b0fd4168e93e10](https://www.huffpost.com/archive/in/entry/copseye-facial-recognition-data-leak_in_5d7255a4e4b0fd4168e93e10)

<sup>72</sup> Kashmir Hill. The Secretive Company That Might End Privacy as We Know It. The New York Times. January 18, 2020. Available at: <https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html>

<sup>73</sup> Gary Smith. High-tech redlining: AI is quietly upgrading institutional racism. Fast Company. November 20, 2018. Available at: <https://www.fastcompany.com/90269688/high-tech-redlining-ai-is-quietly-upgrading-institutional-racism>

<sup>74</sup> Soumyarendra Barik. India's NCRB To Test Automated Facial Recognition System On 'Mask-Wearing' Faces. Medianama. September 25, 2020. Available at: <https://www.medianama.com/2020/09/223-indian-automated-facial-recognition-system-face-mask-detection/>

<sup>75</sup> Artificial Intelligence in Real Estate: Embassy Group to Leverage AI Startup Staqu's Platform Across Its Properties. IndianWeb2. August 4, 2021. Available at: <https://www.indianweb2.com/2021/08/artificial-intelligence-in-real-estate.html>

The ongoing unregulated and invisible collaboration between governments and private corporations, thus, poses serious risks to individual privacy and informational autonomy. More transparency in this partnership, and the establishment of oversight through clear checks and balances, are necessary, if such an arrangement is to continue in a fair and accountable manner. We will broach this further in the final section of this paper.

## Issues surrounding unclear legal liability

The use of FRT in law enforcement poses several risks and each warrants a deeper consideration from a liability standpoint. Arguably, the most insidious risk is to an individual's freedom and liberty, as inaccurate FRT results can result in apprehension, detention, prosecution and even potential conviction of an individual. Again, these are not merely theoretical conjectures - there have been instances of misidentification which have caused detrimental results for innocent individuals.<sup>76</sup>

The issue around legal liability of AI (and its specific manifestations like ML algorithms) is highly debated.<sup>77</sup> While consideration of the nuance of where and how liability can be imputed is a theme for more detailed scholarship, the authors herein are simply aiming to flag the polycentric nature of the ecosystem of law enforcement within which a flawed FRT algorithm can create a legal cause of action against different actors. From a liability perspective there are three main concerns - first, the liability of the private corporation or developer of the FRT algorithm; second, the liability of the state for deploying a flawed algorithm; and third, potential of holding the algorithm liable, per se.

Beyond the debate around who to hold accountable, in India's case, the manner in which FRT has been pursued by law enforcement agencies, there is little recourse for judicial action. Any litigation would require a substantial amount of evidence to establish the liability of both private and state actors. Particularly for private actors, the secrecy offers a de facto immunity from potential legal liability as it is nearly impossible to build a proper case, in the absence of even the most fundamental details of this arrangement. As researchers, the authors have struggled to piece together even some rudimentary aspects of how the state governments have engaged private corporations, governing norms or terms of reference for such an arrangement, and whether there are any liability provisions

---

<sup>76</sup> Victoria Burton-Harris and Philip Mayor. *Wrongfully Arrested Because Face Recognition Can't Tell Black People Apart*. ACLU. June 24, 2020. Available at: <https://www.aclu.org/news/privacy-technology/wrongfully-arrested-because-face-recognition-cant-tell-black-people-apart/>

<sup>77</sup> See for instance Paulius Čerkaas, Jurgita Grigienė and Gintarė Širbikytė. *Liability for damages caused by artificial intelligence*. *Computer Law & Security Review*, 31(3), pp. 376-389. 2015. Available at: <https://www.sciencedirect.com/science/article/abs/pii/S026736491500062X>

governing this relationship. For a potential accused, access to this information will be utterly inaccessible.

What results from this is an arbitrary ecosystem where despite high risks of surveillance, privacy infringement, transgressions against due process, and a real threat to constitutional and legal rights, there is no meaningful recourse. Depriving an individual of proper access to justice in itself violates the sacrosanct ethos of the Indian Constitution and would certainly fall short of the idea of “constitutional morality” that has become the cornerstone of AI ethics in India.<sup>78</sup>

## Private goals drive public priorities

When a significant portion of the technology for facial recognition is provided to public agencies by the private sector, the peculiar motives of private actors affect the development and use of this technology. Consequently, private motives affect public outcomes. In this section, we will use the case of Clearview AI along with other examples to illustrate that often these motives are incompatible with public welfare and can distort public outcomes.

1. Profit, free trials and proliferation: When Clearview AI started out, it followed a model that is by now quite familiar to us: deep discounts for customers to create and capture a market.<sup>79</sup> It offered police departments free trials and cheap licenses at the beginning to demonstrate to the police the value of its technology.<sup>80</sup> This made many policing agencies de facto brand ambassadors of the technology. While there may be nothing wrong with offering discounts to public agencies, this practice in a legal vacuum and in the absence of public deliberation reflects a mispricing of the technology. In effect, not only was the technology deployed without consultation with the public or without a social welfare assessment, it was also deployed at an artificially low price. This is because there is a private interest in proliferation of this technology, which motivates the low price. The private interest was not exposed to a balance with the public interest due to the opacity of the use. In India, several FRT providers are also funded by venture capital and are presumably able to provide this technology at deep discounts.

---

<sup>78</sup> Responsible AI: Part 1 - Principles for Responsible AI. IndiaAI. Available at: <https://indiaai.gov.in/research-reports/responsible-ai-part-1-principles-for-responsible-ai>

<sup>79</sup> Kashmir Hill. The Secretive Company That Might End Privacy as We Know It. The New York Times. January 18, 2020. Available at: <https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html>

<sup>80</sup> Ibid.

The mispricing of the technology leads to use that is well above the socially optimal use. In other words, policing activities are increased and sharpened to unjustifiable levels because the technology is made available for cheap in the short term. Such over-policing can lead to over-criminalisation of society. In 2017, the Times of India reported that the Chennai police approached a “quarrelling group” and used the FaceTagr FRT app on them. It revealed that one of the people had pending cases against them.<sup>81</sup> It is not unclear why this example was considered a success story by the police, or how it would clear any test of necessity and proportionality. Similarly, Staqu’s principal FRT, christened Jarvis, can be used to detect “unnecessary loitering and suspicious activity”.<sup>82</sup> The description on Staqu’s website is accompanied by a picture of a homeless man, clarifying the usual targets of such surveillance [Annexure 3].

Since the phenomenon of over-criminalisation has been discussed in detail in the previous papers in this series, we will not cover it in detail here.

2. Conflicts of interest: Clearview AI scrapes images from social media websites to develop its database. Naturally, Facebook is a major source of image data for Clearview. In February 2020, Facebook demanded that Clearview AI stop using its data, as this activity was in violation of Facebook’s policies.<sup>83</sup> However, a prominent investor in Clearview AI - Peter Thiel - also sits on Facebook’s board.<sup>84</sup> Notably, Facebook, unlike Twitter, did not send a formal cease and desist letter to Clearview AI.<sup>85</sup>

Serious concerns about conflicts of interest are raised when the same people or entities are invested in FRT for law enforcement as well as data gathering for non law-enforcement purposes. In the Indian context, the private entities that are currently, or may potentially design such algorithms for law enforcement agencies, will trigger similar questions. It is also pertinent to state here that the proposed PDP Bill is unlikely to offer much resolution to such conflicts of interest. It currently provides numerous clauses which enable the central government to exempt the application of numerous substantive provisions of the draft bill to

---

<sup>81</sup> A Selvaraj. Cops use mobile app to scan faces, crack cases. *The Times of India*. November 16, 2017. Available at: <https://timesofindia.indiatimes.com/city/chennai/cops-use-mobile-app-to-scan-faces-crack-cases/articleshow/61665626.cms>

<sup>82</sup> Jarvis. See: <https://www.staqu.com/jarvis>

<sup>83</sup> Jon Porter. Facebook and LinkedIn are latest to demand Clearview stop scraping images for facial recognition tech. *The Verge*. February 6, 2020. Available at: <https://www.theverge.com/2020/2/6/21126063/facebook-clearview-ai-image-scraping-facial-recognition-database-terms-of-service-twitter-youtube>

<sup>84</sup> Kashmir Hill. The Secretive Company That Might End Privacy as We Know It. *The New York Times*. January 18, 2020. Available at: <https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html>

<sup>85</sup> Jon Porter, supra at 83.

entities including private corporations, which are deemed necessary for law enforcement.<sup>86</sup> Hence, it is legally conceivable that entities engaged in designing such surveillance technologies for the state are afforded such exemptions on their data processing.

3. Manipulation of data: The New York Times article that first broke news about Clearview AI's activity also showed that the company could manipulate its database and block search results for certain faces.<sup>87</sup> The relevant quote from the article is below:

*“After the company realized I was asking officers to run my photo through the app, my face was flagged by Clearview’s systems and for a while showed no matches.”*

For an activity as sensitive as law enforcement, the ability of a private actor to manipulate the results of a search seems perilous. In the context of India, when the partnerships between private technology providers and police agencies are so opaque, there is very little opportunity to examine the level of control the police exerts over the database, and the transparency with which the technology functions.

The incentives in the use of privately provided FRT in law enforcement are similar to those of private prisons in the United States. Private prisons have been shown to be primary drivers of mass incarceration and the heavily racially biased “war on drugs” in the US.<sup>88</sup> The profit incentive in imprisonment - along with other factors - ends up promoting government action in increasing imprisonment and criminalisation of activities that are either harmless or best reduced through non-punitive measures.<sup>89</sup> In fact, there is now an entire for-profit industry of bail bonds that traps people in debt once they are arrested.<sup>90</sup> The effects extend to foreign policy as well - as of 2016, nearly three fourths of US federal immigration detainees were held in private prisons.<sup>91</sup> The toll of the war on drugs in terms of life years and lives lost is staggeringly high, and should give anyone pause while considering the promotion of private interests in law enforcement.

---

<sup>86</sup> The collective reading of the draft sections 35, 36, and 37 gives broad exemptionary powers to the central government in this regard. See the draft bill at [https://prsindia.org/files/bills\\_acts/bills\\_parliament/2019/Personal%20Data%20Protection%20Bill,%202019.pdf](https://prsindia.org/files/bills_acts/bills_parliament/2019/Personal%20Data%20Protection%20Bill,%202019.pdf)

<sup>87</sup> Kashmir Hill, *supra* at 84.

<sup>88</sup> Private Prisons. ACLU. Available at: <https://www.aclu.org/issues/smart-justice/mass-incarceration/private-prisons>

<sup>89</sup> Banking on bondage: private prisons and mass incarceration. ACLU. Available at: <https://www.aclu.org/banking-bondage-private-prisons-and-mass-incarceration?redirect=prisoners-rights/banking-bondage-private-prisons-and-mass-incarceration>

<sup>90</sup> For-profit bail bonds industry and insurance corporations trap people in cycle of debt. ACLU. Available at: <https://www.aclu.org/press-releases/profit-bail-bonds-industry-and-insurance-corporations-trap-people-cycle-debt>

<sup>91</sup> Private Prisons, *supra* at 88.



To be clear, there are cases of the positive involvement of private providers in public services. But the involvement of private interests in security provision is a special case because it directly affects the coercive actions of the state, which in ordinary circumstances are subject to democratic control. There is a rich literature about the consequences of private incentives driving security provision. Perhaps the most well-known expression of this general relationship is Eisenhower’s phrase “military-industrial complex”.<sup>92</sup> Eisenhower pointed to not only the profit motive and monopolisation of defence markets, but also the difficulty in cutting back spending on these endeavours once it was increased and entrenched.<sup>93</sup> Without undue alarmism, the takeaway for us should be that at the very least, a clear and public examination of the costs and benefits of privately-provided technology for law enforcement should be carried out before its use is entrenched.

---

<sup>92</sup> NPR Staff. *Ike's Warning Of Military Expansion, 50 Years Later*. NPR. January 17, 2011. Available at: <https://www.npr.org/2011/01/17/132942244/ikes-warning-of-military-expansion-50-years-later>

<sup>93</sup> *Ibid.*



# III. Recommendations

---

The issues caused by the private provision of FRT for law enforcement concern both individual rights and public welfare, and manifest in both the short and long term. Accordingly, we recommend the following policy measures to minimise the negative implications of private provision:

## Transparency of agreements

We have demonstrated that there is a clear lack of transparency in the agreements between police agencies and private technology providers regarding the FRT systems in use by the police. This opacity has implications for privacy and data security, and precludes meaningful judicial recourse for people. In the past, information on such agreements has been denied to the public citing an exception related to trade secrets.<sup>94</sup> We recommend that all such agreements be in the public domain and thereby open to public scrutiny. The details that should be in public domain include: the kind of technology being provided, the databases used for training and matching, the accuracy of the technology, the financial details of the agreement, and the liability incurred by all parties involved. In addition, the procurement process for FRT solutions should be transparent from end to end.

## Algorithmic standards and regulation

From the example of Clearview, it is evident that FRT databases and results are open to be manipulated by the private technology provider. Legal standards on algorithmic transparency and performance will help avoid such manipulation by making the workings of the system clearer. There should also exist a set of regulations specifying the ability of personnel from all parties to engage with the data and results, thus minimising the risk of tampering. The said regulations must also consider establishing liability standards for private entities that design such algorithms, and potential vicarious liability for state entities deploying the same.

Robust data protection regime and need for balancing executive action

---

<sup>94</sup> Shouvik Das. Facial Recognition and 'Trade Secrets': What Exactly are Police Forces Doing with Surveillance Tech?. News18. December 4, 2020. Available at: <https://www.news18.com/news/tech/facial-recognition-and-trade-secrets-what-exactly-are-police-forces-doing-with-surveillance-tech-3145223.html>

The upcoming law on data protection must delineate liability for data breaches among all involved parties. It must establish clear obligations for any entity acting as a data processor, to ensure principles of purpose control, proportionality, and public interest are preserved (as established by the Supreme Court in *Puttaswamy*). It must also establish clear checks and balances for state actions in law enforcement and national security, which are likely to impinge on individual privacy and informational autonomy. This too would be in conformity with the Supreme Court's ruling in *Puttaswamy*. The draft PDP Bill of 2019, gives unbridled power to the Central government to exempt state and in some cases, even private entities, from their obligations under the proposed data protection law. This would run afoul of the proportionality test from the said judgment, and would fail to protect against harms of FRT in law enforcement.

## Stricter legal restrictions on surveillance

The Information Technology Act, 2000 through Section 69 contains over-broad provisions allowing for surveillance by the state. While it may be imperative for the state to undertake surveillance functions at times, it is also crucial the same occurs with some form of oversight to prevent arbitrariness. Having a judicial mechanism for any surveillance actions undertaken in pursuit of the IT Act, is a way to balance the interests of the state, and individual rights and liberties. An example of this are the Foreign Intelligence Surveillance courts established in the US under the Foreign Intelligence Surveillance Act (FISA), which are specialised courts tasked for evaluating governmental requests for surveillance activities.<sup>95</sup> It is also crucial that states take regulatory measures at their level, since law and policing are state subjects, and enact adequate legislation to establish checks and balances where such technology is adopted in law enforcement.

## Public involvement in decision-making

The non-privacy related dangers of private provision of surveillance technology, such as that of private interests driving coercive public policy, need to be examined by the people and public representatives. Because of the larger societal implications, a broader public discussion about such technology provision is required before the entrenchment of this provision in India's law enforcement systems. At minimum this involves attempting to attain the sanction of Parliament by introducing a law for FRT; other methods include public consultations, and public investment to build capacity to assess such technologies.

---

<sup>95</sup> Website of the United States Foreign Intelligence Surveillance Court: <https://www.fisc.uscourts.gov/>

Implementing these measures will require coordination between public agencies and private sector providers, and cannot be carried out without the active involvement of people, their representatives, and civil society organisations. These recommendations tie in to our overall recommendations made in the first two papers in this series that attempt to minimise the harms caused by the use of FRT for law enforcement.

# Conclusion

---

Our three-paper series has highlighted the unique challenges posed by the use of FRT for law enforcement purposes in India. The existing pitfalls of FRT, such as inaccuracy and bias, manifest in worrying ways in a law enforcement context. This third paper has shown the implications of the already common involvement of the private sector in providing FRT to law enforcement agencies in India.

The issues caused by the use of technology in policing are exacerbated by the use of privately-provided technology in policing. Private sector involvement can reduce public control over outcomes important to the public as a whole - in this case, opaque and unbridled use of privately provided FRT in law enforcement reduces public control over coercive state activities. The use of FRT is also proliferating out of law enforcement by the state to private security uses, such as by real estate entities. The exceptions of national security and law and order, which are often cited to justify surveillance, can be misused by both the state and private companies to further their own interests in detriment to the public interest.

We accordingly recommend that transparency in FRT agreements, algorithmic regulation, clarity on data protection responsibilities, stricter legal restrictions on surveillance and public involvement in decision making over FRT be implemented to minimise the harms caused by the private provision of FRT for law enforcement.

# Annexure – 1

---

Template of RTIs filed with police agencies:

Specific subject matter of the document	Information regarding the use of facial recognition technology provided by [Company Name]
<i>Further details of queries</i>	<p><i>As reported in [Newspaper Name] on [Date], [Police Agency] has used technology by [Company Name] to monitor people in real time in [Reported Incident]. Please provide the following details and accompanying documents:</i></p> <ul style="list-style-type: none"><li><i>a. A copy of the tender and final agreement signed between [Company Name] and [Police Agency].</i></li><li><i>b. Please provide the formal bidding documents submitted by [Company Name] for being granted this project.</i></li><li><i>c. The cost that is being incurred by the [Police Agency] as payments made to [Company Name] for contributing this technology, and its subsequent upkeep and maintenance.</i></li><li><i>d. Which other private corporations bid for contributing this technology, if any. Please furnish their respective bidding documents.</i></li><li><i>e. Please provide any additional official documents regarding the role of [Company Name] in providing facial recognition or other technology to [Police Agency].</i></li></ul>

# Annexure – 2

Response received from the Public Information Officer, Police Commissioner of Surat to the RTI filed by us:

R.P.A.D

Sample: -c  
(See Rule 4 (1))

Matter of providing information to the applicant and / or denying it.

From: -

No.: -Vahat / K-7 / RTI / 338 / 2021.  
Public Information Officer, and  
Deputy Administrative Officer,  
Office of the Commissioner of Police,  
Surat City. date. 6 / 08 / 2021.

TO.

MR. Jay vipra

ADD.: -A-232 Defence Colony  
New Delhi-110024.

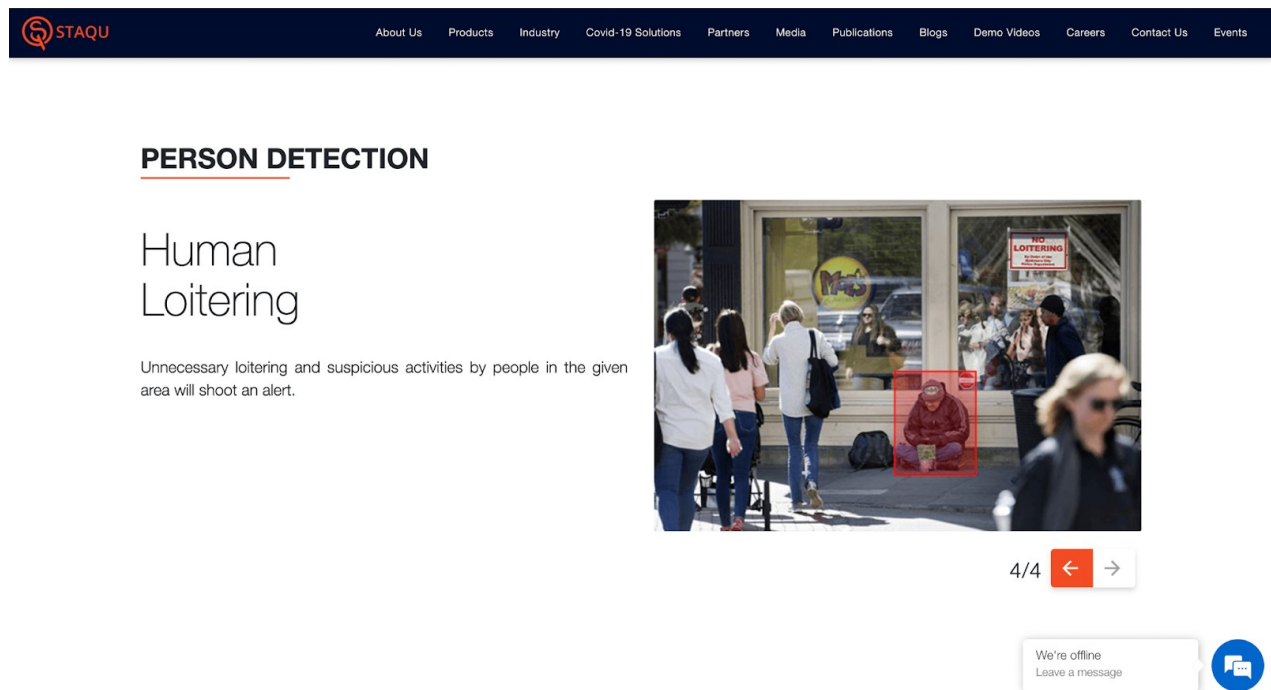
In pursuance of your application dated 08/07/2021 receiving to date-14/07/2021 is requesting to provide information / documents under Right to Information Act, 2005-

No agreement has been signed with NEC by the office here as per the information you have requested.

Public Information Officer and  
Deputy Administrative Officer  
Office of the Commissioner of Police  
Surat city

# Annexure – 3

Screenshot from Staqu's website, described in Chapter III, accessed on December 15, 2021:



The screenshot displays the Staqu website's navigation bar at the top, featuring the Staqu logo and menu items: About Us, Products, Industry, Covid-19 Solutions, Partners, Media, Publications, Blogs, Demo Videos, Careers, Contact Us, and Events. The main content area is titled 'PERSON DETECTION' and includes a sub-section for 'Human Loitering'. The text explains that 'Unnecessary loitering and suspicious activities by people in the given area will shoot an alert.' A video player shows a street scene with a person in a red hoodie sitting on a bench, highlighted by a red bounding box. The video player includes a '4/4' indicator and navigation arrows. A chat widget at the bottom right shows a 'We're offline' message and a 'Leave a message' button.

**PERSON DETECTION**

## Human Loitering

Unnecessary loitering and suspicious activities by people in the given area will shoot an alert.

4/4

We're offline  
Leave a message