FACE SURVEILLANCE AND GOVERNMENT INTRUSION

FACE SURVEILLANCE TECHNOLOGY THREATENS OUR PRIVACY AND BASIC FREEDOMS

Face surveillance technology gives the government **unprecedented power** to track who we are, where we go, what we do, and who we know.

- Face surveillance threatens to create a world where people are watched and identified as they attend a protest, congregate at a place of worship, visit a medical provider, and go about their daily lives.

- Every US city has public surveillance cameras, and many of those systems are connected in regional surveillance networks. With a simple software update, the cameras could be supercharged, serving as nodes in a network of ubiquitous face surveillance.

- Using face surveillance, the government doesn't need to stop and question you to track you in public or to identify you. They don't need personal documents, fingerprints, or your phone — they just need to see your face on camera.

- All this happens at a distance, without your knowledge. You can't refuse this kind of search. You can leave your ID and phone at home, but you can't leave your face.

- Without safeguards, government officials could secretly use face surveillance technology to track every person's every movement in public space—not on one day, but on every day—merely with the push of a button.

FACE SURVEILLANCE TURNS ORDINARY PEOPLE INTO SUSPECTS

Face surveillance technology threatens to create a secret, perpetual lineup — in which ordinary people are implicated without their knowledge.

- Since 2006, the Massachusetts Registry of Motor Vehicles (RMV) has made their driver's license database available to state and federal agencies for facial recognition searches. The RMV never disclosed this information to the public, or waited for legislative approval before allowing these searches.

- This means that millions of people who applied for driver's licenses were not told they would be submitting their biometric information to a database of faces — one that is now being used for government investigations.

- State and federal agencies can request face recognition scans of the RMV's database, which means millions of ordinary people are at risk of being misidentified or deemed suspicious by potentially biased software, without knowing why.

- Until limited restrictions passed in 2020, nobody knew what standards these agencies had to meet for the RMV to grant a face scan request. Now we know, and we know how inadequate they are.