UNCUT-NEWS

INDEPENDENT ANALYSES AND INFORMATION ON GEOPOLITICS, ECONOMICS, HEALTH, TECHNOLOGY

From boarding pass to bio-ID: Airports become the front line of the surveillance state

April 15, 2025.

Part 1: From the boarding pass to the Bio-ID – Introduction and start of the surveillance system

In a world obsessed with rationalization, opting out is no longer part of the travel plan.

It starts with a smile. Not the fake smile you wear at family gatherings, but the forced expression you put on at the airport scanner. Congratulations: Your face is now your boarding pass, your passport, your national identity card, and, if things continue as they are, probably your tax return. The biometric revolution is here, and it's wearing the sleek, sterile uniform of "efficiency."

Gone are the days of clutching a passport like a nervous toddler clutching a teddy bear. The humble little booklet, once the last shred of analog dignity in a digital world, is being replaced by something far more convenient and, coincidentally, far more dystopian. It's called the Digital Travel Pass, and it wants your face. Not metaphorically. Literally.

For more than a century, international travel was simple. Show your ID. Get a stamp. Move on. But apparently, pulling out a booklet became too tedious for the speedy, app-saturated modern traveler. So governments, never one to miss an opportunity to add another layer of surveillance under the guise of modernization, decided to cut out the middleman and scan your biometric soul instead.

The offer is tempting. Faster lines. Fewer documents. No fumbling around kiosks like a bewildered raccoon. Singapore, the eager student of the techno-authoritarian classroom, has already flung its doors wide open. More than 1.5 million people have been funneled through Changi Airport without having to show a single document. Their identities have been confirmed by algorithms trained to recognize tired people slumped in neck pillows.

Not to be left behind, several governments, including Finland, Canada, the United Arab Emirates, and the United States, are playing their own game with biometric data. The digital travel pass, approved by the United Nations International Civil Aviation Organization (ICAO), is currently being piloted. Consider it a global beta test for transforming airports into facial recognition carnivals.

Part 2: Global Tests and the Price of Convenience

The ICAO, ever the champion of dystopian chic, promises that the DTC will create "seamless travel experiences." Authorities can verify a digital representation of passport data prior to the traveler's arrival and confirm the integrity and authenticity of the data. In Finland, the entire check-in process reportedly takes eight seconds.

That sounds almost magical. But as with most magic tricks, success comes at a price. In this case, it's your face, which is permanently stored, compared, tracked, and (hopefully) not sold to the highest bidder.

And if this makes you a little uncomfortable, don't worry. You're not alone. Data protection advocates, those annoying people who constantly harp on about "rights" and "transparency," are sounding the alarm.
Once your biometric data is captured at the airport, it doesn't simply vanish in a puff of digital smoke. It lives on, hidden in databases as secure as a screen door in a hurricane. Different countries have different regulations regarding what can be done with your data. That's a polite way of saying that no one knows where your face ends up.

Smile, you are being processed.

The irony is that while ICAO and its member states are portraying this as a leap into the future, they are actually opening a back door to the past, to a time when governments could track your every move—only now they can do so in high definition and in real time.

All of this is done with the usual cocktail of corporate jargon and government rhetoric. It's not just about making travel easier, it's also about making surveillance feel like customer service. A seamless experience. Just smile for the scanner, collect your luggage, and forget you ever had any privacy.

No one voted for it. That's the funny part. No one held a referendum and asked, "Would you like to trade your fingerprint and your face for the privilege of slightly faster boarding?" It just happened—through pilot programs, technology partnerships, and quiet bilateral agreements that sound like cocktail napkin deals in airport lounges.
By the time the average traveler notices, their face is already stored in a database called “trusted traveler.”

Part 3: Technocracy without consent – the creeping coercion

The beauty of biometric surveillance, from a bureaucratic perspective, is that it easily circumvents democratic input. There's no need to pass a controversial law or engage in a heated debate about civil liberties when you can bury the whole thing under layers of technical jargon and point to improved efficiency metrics.
“Look,” they say, “fewer queues at Heathrow.” Just don’t ask what else has been streamlined.

And let's not pretend this is limited to airports. Once facial recognition becomes commonplace at border control, it will seep outward like a leaky faucet—into train stations, stadiums, shopping malls, and eventually, into your everyday life. The subway barrier that reads your face "for your convenience" also silently logs your commute. Does the retail store use facial recognition to prevent theft? Does it build a profile of your shopping habits.
The line between security and surveillance is dissolving like sugar in tea.

Meanwhile, regulators are playing a game with regulation—always a few years behind the technology and even further behind the companies building them. Governments contract these systems out to private companies and then react with shock when a security breach occurs or when data is monetized in creative, morally flexible ways.

And the public? They're told this is all part of a smarter, safer society.
Don't worry, your data is encrypted. Stored securely. Only authorized personnel may access it.
These are the same promises that preceded every major data breach in the last decade.
If you're wondering whether you can trust the people who stole your Social Security number with your biometric data, the answer rhymes with **"no."**

Part 4: The future is contactless – and consentless

Consent, that tiresome relic of liberal democracy, has no chance in the world of biometric identification. You don't consent. You comply. Or you don't travel.
No real alternative is offered. No physical passport line is labeled "Non-biometric idealists this way."
Just cameras. Gates. And the cheerful beeping that confirms you've been scanned, checked, and placed on the machine.

This is the endgame of convenience culture: a society in which efficiency displaces thought, in which identity is reduced to a code, and in which the instruments of control are disguised as

luxury features. Once the system exists, it will spread. Because that's what systems do.
Ask anyone who lives in a country where protesting too loudly with a flag is punished or persecuted – or worse.

Whether in the boardroom of a company or in a government security agency, the incentive to misuse this data is deeply embedded in the structure. Control is power. Knowing where people are, who they're with, and what they're doing is a tool for exerting pressure. This is surveillance capitalism with a badge.

And now comes the bitter punchline: When enough people notice this, it will be too late to get out.
The infrastructure will be in place everywhere. The databases will be built. The cameras will be installed.
Your biometric ID, already used for everything from boarding an airplane to accessing public services, will de facto be the key to life itself.

You'll smile at the scanner because you have no other choice. And the machine will smile back—not out of politeness, but because it just won.

Part 5: Biometrics in the USA – Lawless space and private gold rush land

Biometric data in the USA: A legal Wild West

The land of the free? Safe—free for corporations and government contractors to take your face, fingerprints, and maybe even your child's thumbprint in the public school cafeteria.
The safeguards? A few scattered state laws, a lot of shrugging, and a set of rules that looks like it was put together during a coffee break at a Silicon Valley hackathon.

Europe—despite its bureaucracy moving at the speed of molasses—has somehow managed to pass the General Data Protection Regulation (GDPR). A far-reaching, but admittedly flawed, regulation that actually treats personal data as if it were important.
On the other side of the Atlantic, the US response was a resounding “Good luck out there.”

Only three states—Illinois, Texas, and Washington—have dared to pass something resembling a biometric privacy law. Of those, Illinois' Biometric Information Privacy Act (BIPA) is the only one that truly makes a difference.
Under BIPA, companies must ask before they capture your face. What a concept. And even better: If they screw up, you can sue them.
Of course, tech companies hate this – with the intensity of a thousand data breaches.

And everyone else? Now it's open season. Your gym can scan your face. Your workplace can record your keystrokes and heartbeat. Your grocery store can track your walk. And if you don't live in one of those three states, there's not much you can do about that data being passed around like a bowl of chips at a Super Bowl party.

This vacuum of government regulation isn't a flaw. It's the business model. Companies like Clearview AI thrive on it. These digital bounty hunters have scraped billions—yes, with a B—of images from the internet to develop facial recognition tools sold to law enforcement agencies. No consent. No disclosure. Just "innovation."

Airports have, of course, become the glittering showroom for this surveillance bonanza. "Public-private partnerships" is the polite term for the arrangement in which government agencies collaborate with private technology companies to develop facial recognition systems. What they don't tell you is how your biometric data might be shared between CBP, TSA, airlines, and who knows what other third-party vendors maintaining servers in Arkansas.

No federal law means no mandatory expiration date, no clear earmarking, and no real accountability.
Your face could board a plane in Atlanta and appear in a Nevada law enforcement database two years later.
Don't ask how it got there. They'll tell you it's "secret."

Part 6: The creeping function – how biometrics mutate into total control

Creeping function: When biometric convenience becomes a surveillance trap

Once your face is in the system, it usually stays there. And not just for the reason you were told. This is the essence of creeping function—the bureaucratic sleight of hand where a tool introduced out of convenience becomes a Swiss Army knife of surveillance.

Initially, facial recognition was sold to travelers as a clever time-saver. Scan and go.
But now those same systems are being linked to crime databases, immigration records, and intelligence watch lists.
What began as a convenience at the gate is becoming a digital search network – with you at the center.

The U.S. Customs and Border Protection agency acknowledges that images collected during travel may be shared with “other government agencies.”
That's government language for: We don't have to tell you who, why, or for how long.

In India, this tech hype has been taken to a new level. The **Digi Yatra** program, billed as a "voluntary" biometric boarding system, is casually being expanded to hotels and tourist attractions. Because when checking into a cultural landmark, you really want the same security system as at the airport.

This is no exception. It's the way things are. The biometric infrastructure is designed to grow.
One minute it is used to speed up processing.
The next moment it is determined who has taken part in a demonstration, whether a tenant is behind on the rent or whether a student has skipped class.

The technology doesn't creep in. It spreads. It metastasizes.
And without fixed legal limits, it will continue to spread into every corner of social life.
All this, of course, under the sweet guise of “rationalization” and “user-friendliness.”
Tech companies are allowed to innovate. The government is allowed to monitor. They can give retroactive consent.

Part 7: One face, endless uses

One face, endless uses

The insidious function thrives in silence.
Most people don't realize that by agreeing to a facial scan at the airport, they are also agreeing to the indefinite storage of their biometric data - which is stored God knows where.
They are not told whether this data will be deleted, shared or sold.
Because no one wants to admit that once their face is recorded, it becomes a permanent access point to their identity.

This is the great bait and switch of biometric convenience:
It sells you freedom of movement – and at the same time provides the architecture of surveillance.
It promises personalization – and at the same time delivers profiling.
It offers speed – while extracting your most intimate identifiers for use in systems you can't see and wouldn't consent to if you could.

Without enforceable limits and real accountability, biometric technology will not stop at the airport.
It will follow you into schools, offices, shops, parks – and ultimately into the structure of your daily life.

And if you ever dare to fight back, the cameras will be watching.

You cannot opt out of a society where your body has become your ID card.
One can only hope that those in charge remember that rights matter – even if you are just trying to get a flight.

Part 8: Biometric Glitches – When Machines Ruin Lives

Biometric Glitches: When Technology Misunderstands Your Face—and Your Identity

Facial recognition is touted as a marvel of modern efficiency: no ID, no problem, just scan and go.
But behind the curtain of high-tech magic lies a system that still cannot reliably distinguish one person from another.
And when it's wrong, the consequences don't look like a harmless software hiccup. They look like handcuffs.

These systems are based on the assumption that a few billion faces are just unique barcodes waiting to be captured.
In reality, they are clunky, error-prone, and completely overwhelmed by their own precision.
It's one thing if your phone doesn't recognize you before coffee. It's another if an airport scanner decides you don't exist—or worse, that you're someone else entirely.

An example:
A man in Detroit is arrested after a facial recognition system mistakenly identified him as the suspect in a surveillance video.
The machine makes the decision – and suddenly you are explaining your whereabouts to a very humorless police officer.
30 hours later, the system admits its mistake, but it is not the machine that spends the night in a cell.

These symptoms are an expression of a broader problem:
Systems designed for mass identification are unable to consistently identify individuals.
At the border, this leads to delays, second screenings and missed flights.
In other areas of life, it can mean being flagged, rejected, or arrested by a machine that thinks you are someone you are not.

The underlying problem is very simple:
These tools are trained on huge datasets, often gathered from cheap and easily accessible sources.
No one checks the process. No one asks what happens if the system is wrong—because algorithms apparently cannot be held accountable.

Technology companies are bringing these systems to market as if they were selling a new lemonade: lots of hype, little responsibility.
They'll assure you that the next update will fix the problem. They'll say that accuracy is getting better and better.
What they won't say: what happens if the wrong person is tagged - and a human approves the result because "the computer said so."

It is a failure of administration as well as a technical failure.
Machines make important decisions about who gets on planes, who gets taken aside, and who gets arrested.
And they do this without any transparency, without legal recourse – and often without a second glance from the people they are supposedly monitoring.

This is institutional laziness wrapped in digital mysticism.
And the more we rely on these systems, the more we normalize a world where it's perfectly acceptable for software to mistake your identity—and for you to live with the consequences.

Part 9: Deterrence through surveillance – how freedom disappears from everyday life

The chilling effect of being monitored: How biometric surveillance distorts public life

Surveillance doesn't have to be loud to be effective.
It doesn't have to knock on your door or show up in your inbox.
It just has to exist quietly and silently – without being seen.
This is the new architecture of public life:
A camera in every station. A scanner at every gate. A watchful eye where you least expect it – making you behave a little more... predictably.

You feel it, even if you don't see it.
The nagging feeling that you are being watched makes you walk more upright.
You think again about the joke you wanted to tell.
You might hesitate to join a demonstration or skip a meeting just in case someone is counting.
This is the deterrent effect in action:
Not the fear of doing something wrong, but the fear of being misunderstood by a system that neither forgives nor forgets.

Public spaces are being retrofitted with surveillance systems ,
that not only record, but also interpret – and decide,
who belongs, who acts “suspiciously” and who might be worth taking a closer look at.
The effect is subtle but corrosive. People withdraw.
They avoid risk. They adapt—not out of guilt, but out of caution.

A town square used to be a place of expression, debate and spontaneity.
Now it is a monitored zone where behavior is silently curated by software.
And if each camera is linked to a system that records and tracks you in real time,
public life feels less like a right – and more like an idea.

The real damage lies not only in privacy – but also in participation.
Surveillance, especially when combined with biometric systems, creates a climate
in which people no longer act freely.
They play it safe. They edit themselves.
And finally, the pulsating noise of a free society fades into a controlled murmur.

This is the part that appears in the press releases of the companies,
that sell “intelligent security solutions” is rare.
You'll talk about safety. You'll use words like "efficiency" and "innovation."
They will not mention what happens when everyone in public starts
to act as if he were walking through an airport terminal: **forever.**

Biometric surveillance doesn't just change how we are seen.
It also changes how we live.
And if that's the compromise, then the question is not whether we need better technology.
The question is: **Do we even remember what public freedom felt like before every street corner was monitored?**