Body scanners are used at airport border crossings as an extra security-screening process.

# Protect rights at automated borders

**Gemma Galdon Clavell** calls for checks and balances to avoid the indiscriminate sharing of personal data.

In 2013, the European Union proposed expanding and harmonizing automated border crossings across the region. This Smart Borders initiative could soon be approved[1]. The automated gates (e-gates) in place in many EU airports are the first phase. The European Agency for the Operational Management of Large-scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA) is testing how to link them to databases and processes region-wide. Entries and exits will be stored in a database, replacing passport stamps. This information will be made available to border-control and immigration authorities, and will be linked to fingerprint records and watch lists held by police, customs and immigration agencies.

Around the world, such technologies are transforming the nature of regional and national borders in radical ways. Booths that recognize people's irises, faces and fingerprints are proliferating at airports, ports and other checkpoints. E-gates that compare identities against biometric records stored on chips in passports are supposedly faster, cheaper and more reliable than human border guards, and are presented as technical add-ons to the existing system. But, unmanaged, such technologies can threaten human rights and open up new forms of discrimination.

When our personal data are collected and shared before we board an aeroplane, a border ceases to be a line that separates countries or administrative areas. It becomes a process of monitoring, control and automated decisions. The physical border is increasingly irrelevant because our rights, privileges, relations, characteristics and risk levels are checked all the time.

When booking a ticket with an airline or agent, travellers enter biographical and

DPA/ALAMY

contact details, credit-card information, frequent-flyer numbers, passport information and meal choices into a computer reservation system. A 'passenger name record' is generated and shared among operators. Police and law-enforcement agencies can access these records and check them against police lists, visa databases and fingerprint records to find missing persons, cases of visa fraud and people who have crossed external borders in an irregular way.

People's rights to travel are examined against visa records and 'no-fly' lists. Airlines and authorities look for red flags, identifying individuals who have unusual travel patterns, behaviours or records. Passengers can be physically searched or X-rayed at airports. Facial characteristics and fingerprints are confirmed against digital records on arrival. For individuals entering a country for a period on a visa, data processing continues until their file is closed with an exit record. Alerts are triggered for those who overstay. Hand-held fingerprint scanners and other surveillance methods extend border control, verification and database querying to every corner of a territory to determine who has the right to be there (see 'Big-data border').

For the past three years, my consultancy Eticas has studied the political, policy and social implications of the Smart Borders initiative in collaboration with the European Commission, the European Union Agency for Fundamental Rights in Vienna and the security industry.

We have interviewed and surveyed experts, travellers, border guards and embassy personnel in more than ten countries and observed border-crossing points. Our results have appeared in internal EU documents and policy papers.

We have been startled by the lack of serious assessment, evaluation, risk analysis or attempt to foresee the potential impacts of such changes. Technologies and finance are the EU's main concerns. The human rights, civil liberties and societal implications of securing borders through data processing, mining and matching are receiving little consideration.

There are already warning signs. When a citizen enters their country of origin, national and EU laws establish that person's right not to come under suspicion without serious cause. However, automated borders treat everyone as a potential threat, meaning that these hard-won legal guarantees are ignored.

Travellers give away their data and biometrics to authorities with little awareness of data-protection rights. Processing of these sensitive data is often outsourced to private companies without proper oversight or audits for data security. Meanwhile, border guards are demoted to queue managers, unable to help travellers because they have received little training or information about the new system.

## CITIZENSHIP TEST

E-gates need to discriminate between those who can or cannot cross a border on the basis of their citizenship, permissions to travel and the risk they might pose to their destination country. Legal systems clearly distinguish the data processes that can be applied to citizens and non-citizens[2]. Citizens are specially protected from suspicion on a systematic basis.

Across Europe's Schengen Area, where border checkpoints have been dismantled to allow free movement between countries, the Schengen Borders Code states that citizens returning from non-Schengen areas should undergo a minimum check to establish their identities. This should consist of "a rapid and straightforward verification" that consults "information exclusively on stolen, misappropriated, lost and invalidated documents" to confirm the validity of the travel document (see go.nature.com/2lm8ku4). Border guards may consult security databases only on a "non-systematic basis". Yet automatic checks are by definition systematic. Travellers do not know which checks are performed and why, nor whether their right to avoid suspicion is being upheld.

The Schengen code also states that border guards shall "respect human dignity", "shall not discriminate" and shall take measures that are "proportionate". These qualities are difficult to translate into engineering or computing systems. Difficult, but not impossible: Eticas has been working with companies and institutions to ensure that data processes meet legal requirements and do not disadvantage or discriminate against certain groups. Such complex matters cannot be left to technology providers alone.

Our work suggests that automated border crossings mirror social stratification and inequalities elsewhere. We surveyed more than 1,500 passengers and conducted focus groups with border guards at two airports. We also observed interactions and interviewed travellers and staff at 18 border-crossing points, embassies and visa offices. Border guards reported people reacting to automatic gates in different ways. Frequent travellers — usually young or middle-aged, affluent and technically savvy — are happy to use them and have few problems. Older people and occasional travellers are more cautious. Many elderly passengers declined to answer our questionnaire, for example. Several said that they 'don't understand technology' and, if accompanied by a younger person, passed the survey to them.

*"Travellers do not know which checks are performed and why."*

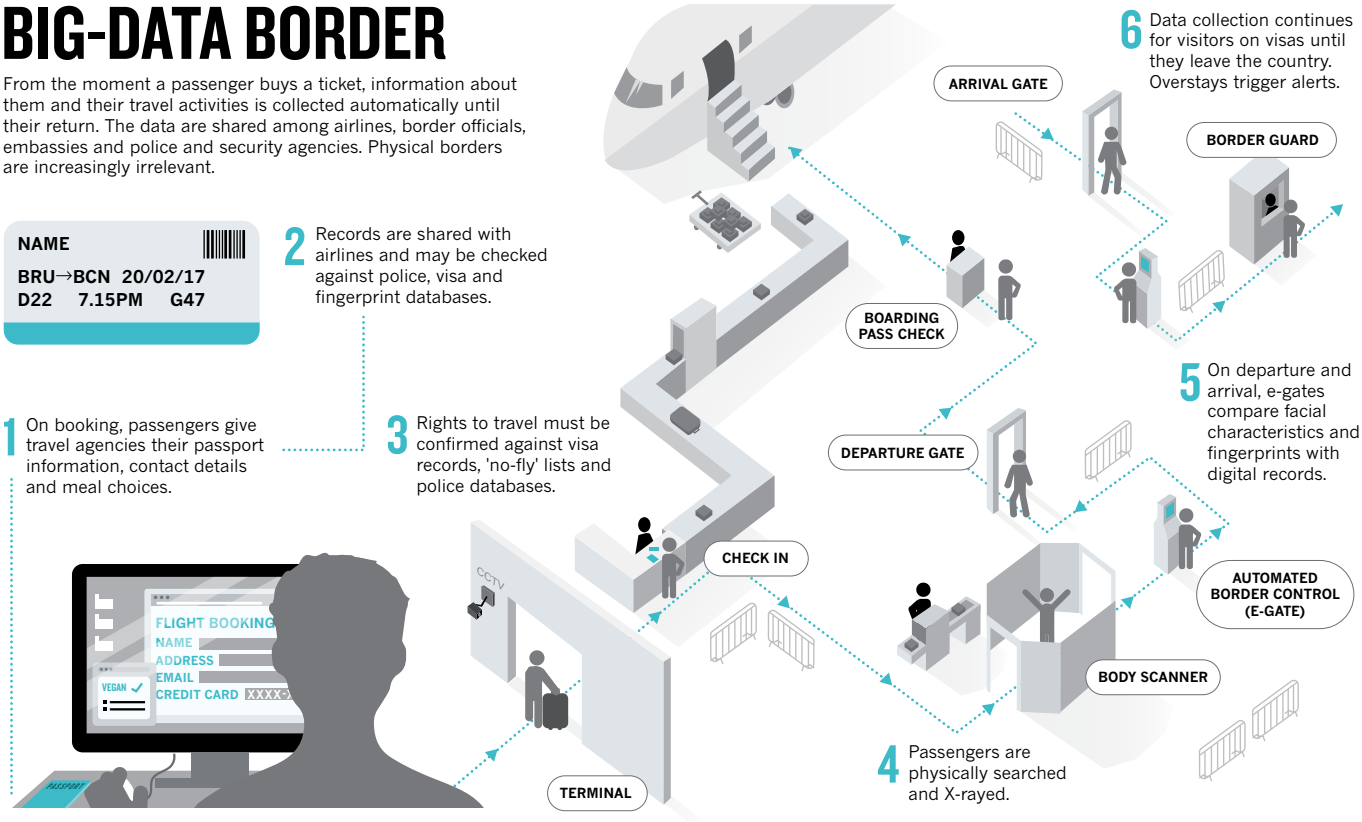
The signage for e-gates is often inadequate and confusing. Guards said that passengers facing the gates for the first time often ask why they need to leave their fingerprints, and want to know what they are going to be used for. These issues stem from the design of e-gates and their intended use primarily for experienced travellers. Bias is introduced at the start — this group benefits over others in terms of time saved and flexibility.

Our research confirmed a trend towards a two-tiered border policy. The crossing process has become an extension of the premium seating classes on the aircraft. Restricted areas for those who can afford them are proliferating, such as VIP lounges and priority lanes for check-in, passport control and boarding. Those who can pay for and access quicker processes can opt out of airport common areas — and even our research. We were not allowed into VIP areas or priority lanes, for instance.

In most cases, monitoring people's movements through digital data — or 'dataveillance' — is about keeping gates open rather than closing them. Bona fide travellers should have a seamless experience, free of queueing and distrust — but that is the case only if they preregister to share their personal data and pay for the privilege[3].

# BIG-DATA BORDER

From the moment a passenger buys a ticket, information about them and their travel activities is collected automatically until their return. The data are shared among airlines, border officials, embassies and police and security agencies. Physical borders are increasingly irrelevant.




ETICAS/CLAIRE WELSH/*NATURE*

Preregistered traveller programmes, set up by border authorities, airlines and airport operators, create the expectation that wealth can buy the right to avoid suspicion. Just as travellers who pay a premium do not have to wait in line to board the aircraft, they might expect not to wait long for a security check.

Discrimination through privilege on the basis of wealth and personal data-sharing raises concerns about human rights, due process and democratic practice (can fundamental rights be bought?), while creating inequalities among citizens when travelling.

## MACHINES AND TRUST

The human and machine components of borders cannot be separated. Guards and travellers are influenced by the technology, and vice versa. Travellers told us that they found interacting with a machine less aggressive than being evaluated by an official. They believed that automated systems are less likely to discriminate. Border guards also welcomed the impersonal and neutral nature of e-gates, but stressed the importance of the "human touch" in identifying suspicious behaviour. For instance, machines have failed to detect some cases of fraud, such as passengers who used another person's passport, and have mistakenly identified a portrait on a T-shirt as the traveller's face.

One of the main concerns among passengers is their right to pass through the border when machines and technology do not work. A mistake in their personal data would be hard to correct, they fear. In interviews at embassies with visa staff who input traveller data, we found many issues that have not been properly taken into account in the flows of data used for decision-making at e-gates. The transcription of names written in non-European alphabets is problematic, as is updating databases with names altered through marriage, for instance.

Whereas people know how to negotiate with another person if they feel they have been wrongfully accused, and thus seek redress, such processes do not yet exist for false positives generated by technology. People feel uncertain and powerless when a machine makes a decision they cannot understand or control. This is happening increasingly as more border crossings implement biometric controls. As long ago as 2007, cases of false positives had become so common at biometric controls in the United States that a Traveler Redress Inquiry Program was set up for affected travellers (mainly those misidentified as being on no-fly lists).

Failing to address these issues lowers citizens' levels of trust in border guards, the state and its automated data processes.

## MOVING FORWARD

Our fundamental rights are at stake when we cross a border. Citizens in the EU and elsewhere need to be able to hold data processes accountable. Governments and the private sector need to make data collection and circulation more secure and transparent. Governments, lawyers, social scientists and technology suppliers should incorporate rights and values into the algorithms and systems used at borders. Privacy-enhancing technologies, policy and risk assessments and acceptability studies can all contribute.

The societal impacts of automatic border crossings need to be assessed for all, from border guards and travellers to member states and society at large. New forms of discrimination arising in data-rich environments need to be flagged and addressed. Channels for redress when systems fail or make mistakes need to be developed. Border guards should receive more training, and staffing should be reviewed. E-gate signage should be clearer. The tools exist to make all these improvements.

We cannot afford to roll out smart borders without taking into account their legal, social and ethical implications. ■

**Gemma Galdon Clavell** *is the director of Eticas Research & Consulting, Barcelona, Spain.*
*e-mail: gemma@eticasconsulting.com*

1. Hayes, B. & Vermeulen, M. *Borderline: The EU's New Border Surveillance Initiatives* (Heinrich Böll Foundation, 2012).
2. van der Ploeg, I. & Sprenkels, I. in *Migration and the New Technological Borders of Europe* (eds Dijstelbloem, H. & Meijer, A.) 68–104 (Palgrave, 2011).
3. Aas, K. F. *Theor. Criminol.* **15,** 331–346 (2011).

G.G.C. declares competing financial interests: see go.nature.com/2lnj8wt for details.