



PENN IUR SPECIAL REPORT

Surveillance or Safety?

How Cities are Rewriting Tourism

BY MAURICIO RODAS, LUKE CAMPO, AND EUGENIE BIRCH

NOVEMBER 2025

MATCH

Photo by Gorodenkoff via Adobe Stock



About the Authors

Mauricio Rodas, Visiting Scholar, Penn Institute for Urban Research, University of Pennsylvania; Former Mayor of Quito, Ecuador.

Luke Campo, Research Associate, Penn Institute for Urban Research, University of Pennsylvania.

Eugenie Birch, Nussdorf Professor of Urban Research and Education, Department of City and Regional Planning; Dean, Graduate Studies, Weitzman School of Design; Co-Director, Penn Institute for Urban Research, University of Pennsylvania.

Acknowledgements

This white paper reflects the collective efforts of a diverse group of stakeholders dedicated to promoting the responsible and effective use of artificial intelligence in urban tourism safety, from policy design and planning to implementation, evaluation, and continuous improvement.

We are grateful to Andrea Vivero, Managing Partner at Meridio Consulting, whose research, insights, and analytical contributions shaped the frameworks and recommendations presented in this white paper.

We also thank the experts who generously shared their perspectives through interviews and consultations: Kevin Werbach, Director of the Wharton Accountable AI Lab at the University of Pennsylvania; Rashid Mukjani, Researcher at the University of Montreal; Natalia Bayona, Executive Director of the UN World Tourism Organization; Jon Berroya, Director of Public Policy and Government Affairs at Google; and Edward Parkinson, President of Public Sector at RapidSOS. Their combined expertise in AI governance, urban policy, tourism management, and technology innovation has significantly enriched this work.

The views expressed herein are those of the authors and do not necessarily represent the official positions of any contributing organizations or individuals.



Table of Contents

Executive Summary	4
I. Introduction	6
II. Tourism and Urban Safety in the Age of AI	8
The Importance of Safety for Tourism	8
Cities at the Intersection of Safety and AI	9
The Critical Challenges	10
The Strategic Opportunity	12
The Evolution of Data & AI Policy	13
Regulatory Environment	15
III. Surveillance Technologies and Alert Systems	17
Public Transparency and Privacy Requirements	18
IV. Cities at the Frontier of AI Tourism Safety	20
V. AI in Practice: City Implementation	23
Case Studies	26
London: AI for Transit Safety and Enhanced Policing Systems	26
Barcelona: Leading on Ethical AI Governance	27
Helsinki: Transparency and International Collaboration	28
Singapore: AI-Enhanced Tourism Safety	29
Miami: Training AI-Enabled Public Safety Officers	30
VI. The Way Forward	34
AI Tourism Safety 10-Point Policy Roadmap	35
Conclusion	37



Executive Summary

Tourism is a cornerstone of urban economies; however, rising concerns over crime, scams, and safety in transport hubs increasingly undermine traveler confidence. Cities are turning to Artificial Intelligence (AI) as a transformative tool to enhance safety through predictive analytics, real-time monitoring, and rapid response systems. At the same time, AI deployment raises pressing governance questions: how to protect privacy, ensure transparency, mitigate bias, and maintain public trust while safeguarding both residents and visitors.¹

Despite AI's promise, cities face a significant implementation gap. Nine out of ten mayors globally want to integrate AI into city management, yet only 2% are actively deploying such systems, according to a Bloomberg Philanthropies survey.² Municipal adoption often outpaces regulatory guidance, leaving gaps in accountability, ethical oversight, and citizen engagement. While national and supranational frameworks such as the EU AI Act, GDPR, and California Privacy Rights Act, offer starting points, cities must develop local policies that address tourism-specific safety challenges, human rights concerns, and the protection of non-citizens.³

This paper examines how cities can deploy AI public safety infrastructure responsibly in tourism contexts. AI-powered video surveillance represents the primary technological infrastructure for threat detection, utilizing dome cameras, pan-tilt-zoom systems, and edge computing analytics that automatically detect suspicious behaviors, abandoned objects, and crowd anomalies. However, effectiveness depends not merely on technological sophistication but on transparent governance frameworks. Privacy regulations across jurisdictions generally mandate clear signage, data minimization, and public notification about surveillance activities. Cities must balance physical security through enhanced detection, digital protection through secure data practices, and psychological safety through transparent communication that builds visitor trust.

Case studies from London, Barcelona, Helsinki, Singapore, and Miami illustrate diverse approaches to AI deployment in tourism safety. London demonstrates operational efficiency gains in transit monitoring while grappling with facial recognition controversies.⁴ Barcelona exemplifies governance-first adoption through structured ethical oversight. Helsinki pioneers radical transparency via public AI registers.⁵ Singapore showcases strategic public-private partnerships for mega-events.⁶ Miami highlights workforce development for AI-assisted policing.⁷ These experiences reveal common success principles: establishing governance frameworks before large-scale deployment, implementing transparency mechanisms, protecting physical, digital, and psychological safety dimensions, engaging multiple stakeholders, and maintaining continuous evaluation.



The AI Tourism Safety 10-Point Policy Roadmap, the central contribution of this paper, provides a strategic blueprint for destinations aiming to harness AI to enhance tourism safety while effectively managing associated ethical, operational, and governance risks. It proposes a step-by-step approach encompassing the establishment of governance and oversight mechanisms prior to deployment, rigorous data protection and privacy safeguards, transparent decision-making, and continuous accountability. The Roadmap also emphasizes building institutional capacity, fostering public-private collaboration, ensuring inclusive stakeholder engagement, and promoting AI literacy among tourism and public safety professionals.

The paradigm shift from technological capability to governance quality reshapes destination competitiveness. Cities that successfully integrate AI technologies with robust governance will protect residents and visitors, enhance traveler confidence, and gain competitive advantage in global tourism markets. As AI capabilities advance, the differentiator will not be technological sophistication alone but the governance structures that ensure ethical, accountable, and effective deployment. Cities embracing this balanced approach will set standards for responsible innovation, demonstrating that security and civil liberties can coexist when technology serves clearly defined public interests.



I. Introduction

Cities are entering a period of accelerated transformation as artificial intelligence becomes integrated into the systems that shape urban life. From transportation and public safety to tourism and communication, AI is redefining how local governments plan, operate, and engage with both residents and visitors. For tourism destinations, this technological evolution presents both promise and complexity. The challenge is not only to improve operational efficiency and safety but also to maintain fairness, transparency, and trust in how AI systems are designed and deployed. This transformation is unfolding at an unprecedented pace, driven by post-pandemic digital acceleration, rising global travel volumes, and growing expectations for safer and smarter destinations. The convergence of AI innovation and renewed tourism recovery makes this a critical inflection point for city leaders worldwide.

This issue is increasingly urgent because safety has become one of the most decisive factors influencing travel behavior. As visitors rely more on digital platforms and urban infrastructure during their trips, their perception of safety extends beyond physical protection to include digital and psychological dimensions. Destinations that fail to provide visible, credible, and respectful safety systems risk eroding visitor confidence, damaging reputation, and ultimately becoming less competitive in the global tourism market. The urgency is magnified by the expanding use of surveillance technologies, biometric systems, and predictive analytics in public spaces, often advancing faster than regulation. As governments race to balance innovation and ethics, cities now occupy the front line of implementing global AI principles in local contexts.

At the same time, public perception of AI in safety contexts remains mixed. While many recognize its potential to prevent crime and improve emergency response, others question how data is collected, stored, and shared. High-profile debates around surveillance, bias, and privacy have made citizens and travelers more cautious about cities that deploy advanced monitoring systems without clear governance or communication. This heightened scrutiny means that cities cannot rely on technology alone to build trust. They must demonstrate that AI systems are governed by ethical principles, legal safeguards, and accountable oversight mechanisms that protect everyone equally, including temporary visitors.

The use of AI in tourism safety therefore raises broader questions about how cities define security in a digital era. Effective protection now requires balancing three interrelated elements: physical safety through responsive policing and infrastructure, digital safety through secure data practices, and psychological safety through transparent communication that fosters trust.



Cities that treat these dimensions as interconnected are better positioned to enhance both actual and perceived safety. Importantly, addressing these questions now is essential because early decisions on AI governance will set long-term precedents for transparency, inclusion, and international trust. Cities that lead today can shape emerging global norms for responsible tourism technology.

This white paper is organized to guide policymakers, city leaders, and tourism authorities through the key dimensions of AI-enabled tourism safety. It begins by examining the evolving relationship between tourism, safety, and artificial intelligence, followed by an analysis of the global policy and regulatory environment that shapes responsible AI use. Subsequent sections assess surveillance technologies and transparency requirements, explore leading city case studies from London, Barcelona, Helsinki, Singapore, and Miami, and identify comparative insights and global best practices. The paper culminates with the AI Tourism Safety 10-Point Policy Roadmap, which provides a practical framework for destinations seeking to balance innovation, governance, and public trust in the deployment of AI for safer and more resilient tourism environments.

Ultimately, the timeliness and importance of this research lie in its call for proactive governance—before AI adoption becomes irreversible—to ensure that innovation enhances both safety and civil rights.



II. Tourism and Urban Safety in the Age of AI

The Importance of Safety for Tourism

Travel and tourism are major drivers of economic growth, contributing \$10.9 trillion to the global economy in 2024, approximately 10% of total global GDP.⁷ The sector is responsible for roughly 357 million jobs worldwide, which equates to 1 in 10 jobs. International tourism remains the key driver of growth, with total spending by international travelers increasing by 11.6% year-over-year in 2024, more than double the rate of domestic tourism.⁸ In 2024, there were 1.5 billion international tourist arrivals, with this number expected to expand at a rate of 7% annually through 2034.

A key focus of countries seeking to maintain and expand their travel and tourism industries is ensuring the safety of international visitors. Traveler preferences reflect that this should be a top priority, with the Ipsos 2025 Holiday Barometer showing that 32% of travelers consider safety to be the primary factor for choosing a destination, up from 23% in 2021.⁹ Travelers from Europe, North America, and Australia view safety risks as essential to their travel decisions, with 57%, 48%, and 49% respectively citing it as a key factor.¹⁰

Several recent examples highlight how perceived safety and security levels underpin national tourism industries, and how countries can suffer significant economic consequences when these falter. Nepal, for example, which relies on tourism for 8% of its GDP and welcomed 1.2 million international tourists in 2024, saw a 30% year-over-year drop in international visitors this September due to the outbreak of civil unrest.¹¹ Costa Rica has similarly faced challenges in recent years, with a reported 6,300 tourist-related crimes since 2020, causing the United States Embassy in San José to issue a level 2 travel advisory for the country in December of 2024. Several European embassies in the country followed suit, and the economic damage is already being felt, as 2025 is expected to see a 15-20% decline in total tourists as compared to 2024. This presents a significant economic challenge for a country where the tourism sector employs over 500,000 people, contributed \$5.4 billion to foreign exchange earnings in 2024, and accounts for nearly 9% of the national GDP.¹²

Academic research and policy analysis define tourist safety through three interconnected dimensions: physical, digital, and psychological. Physical safety addresses direct threats to visitor wellbeing, including crime, violence, transportation accidents, natural disasters, and public health emergencies. Many destinations prioritize this dimension, as incidents involving theft, harassment, or unsafe infrastructure can have lasting reputational consequences, particularly for cities hosting major events or experiencing seasonal visitor surges. Effective physical safety management requires robust emergency response systems, visible law enforcement presence, well-maintained infrastructure, and proactive risk mitigation strategies that protect both residents and visitors.



Complementing these tangible security concerns, digital safety has become increasingly critical as travelers rely on technology platforms for booking, payments, navigation, and communication. This dimension encompasses protection from cyber threats, data breaches, digital fraud, identity theft, and misinformation that can compromise visitor experiences and personal security. The proliferation of smart city technologies, contactless services, and digital tourism platforms has expanded vulnerabilities while simultaneously creating opportunities for enhanced protection through advanced monitoring and response systems. Destinations must therefore ensure secure digital infrastructure that safeguards traveler information while enabling the seamless technological experiences modern tourists expect.¹³

Beyond these objective security measures, psychological safety encompasses the perceived sense of security and trust that visitors experience throughout their journey. This dimension includes confidence in local law enforcement, the reliability of emergency communication systems, and the broader social atmosphere of inclusion and respect. Psychological safety extends beyond measurable risk assessments to capture subjective perceptions of well-being and belonging. Even when statistical crime rates remain low, perceived insecurity, stemming from inadequate lighting, unfamiliar environments, language barriers, or experiences of discrimination, can deter travel and diminish demand. Consequently, strengthening this dimension requires attention not only to tangible security measures but also to intangible elements such as destination atmosphere, community attitudes toward visitors, and inclusive practices that foster positive experiences across diverse traveler populations. Together, these three dimensions – physical, digital, and psychological – provide a comprehensive analytical framework for understanding and addressing tourist safety in contemporary destinations, forming the conceptual foundation for the analysis presented in this paper.

Cities at the Intersection of Safety and AI

In an increasingly urbanized world, cities play an expanding role in the global tourism industry. Today, approximately 55% of the global population, or nearly 4.5 billion people reside in cities.¹⁴ Major cities around the world represent some of the most iconic international tourism destinations, welcoming tens of millions of foreigners annually. Key examples include Bangkok, with 32.4 million annual visitors in 2024, Istanbul (23 million), London (21.7 million), Hong Kong (20.5 million), and Paris (17.4 million).¹⁵

In most cities around the world, local authorities assume direct responsibility for the safety of residents and visitors through municipal police forces, public transit systems, emergency medical services, fire departments, disaster preparedness and response teams, public health initiatives, street lighting, community outreach programs, and the maintenance of public spaces such as parks and plazas. Around the world, city governments continue to adopt AI to enhance their ability to serve residents and tourists, reducing crime and fatalities, and contributing to a generally safer environment.¹⁶



By their nature, city governments are closer to residents, more in tune with their needs, and therefore better equipped to develop policies that respond to local contexts. Cities, in many cases, can also be nimbler, launching initiatives, policies, and regulations more efficiently than is possible through national-level mechanisms.

The Critical Challenges

Cities face critical challenges in deploying AI responsibly, including balancing technological advancement with robust governance, ensuring the ethical use of data, and protecting both citizens and visitors in an environment of rapid innovation and growing safety concerns.

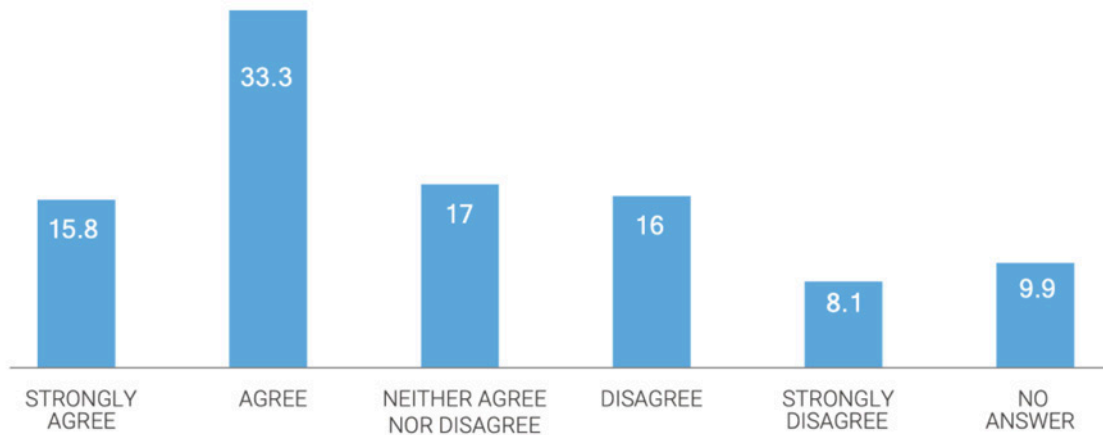
Tourists are increasingly prioritizing safety when choosing travel destinations.¹⁷ In cities with high crime rates or reported incidents involving foreigners that hinder tourism, city leaders may be inclined to step up safety measures to improve the city's image both domestically and globally, while seeking to drive tourism growth.

Deploying AI without adequate governance frameworks exposes cities to material risks, including data privacy violations that breach national or regional laws, potential legal challenges stemming from algorithmic bias and disproportionality, and impacts on vulnerable populations such as minorities, ethnic groups, and individuals with disabilities, who may face discrimination. As academic research confirms, these concerns are not merely theoretical but reflect documented patterns of bias in algorithmic systems.¹⁸

Furthermore, implementing AI without clarity regarding municipal processes for collecting, analyzing, and managing data can create significant rifts with the broader public. A global survey conducted by the UN Interregional Crime and Justice Research Institute found that less than half of all respondents believe AI systems are “essential for solving certain crimes and can support the police to better perform their duties”.¹⁹ Two-thirds of respondents stated that the general public should be informed when AI is used for the prevention, detection, and investigation of crimes.²⁰ Cities must therefore navigate a dual challenge: addressing legitimate skepticism about AI's necessity and effectiveness while meeting rising public expectations for transparency and meaningful communication regarding its deployment in public safety operations. Furthermore, less than half of respondents agreed or strongly agreed that their respective local or national police respected the law and citizens' rights, highlighting a key gap in trust.²¹

Figure 1

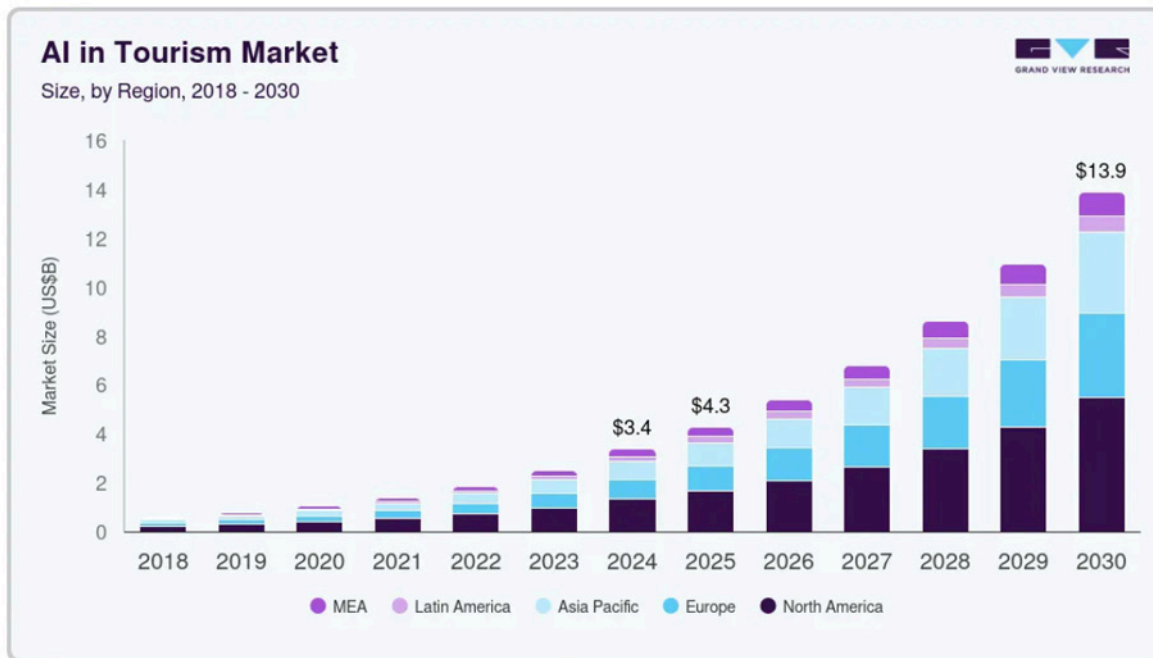
**My local or national police respect de law and citizens' rights
(Percentage of total)**



Source: UN Interregional Crime and Justice Research Institute (2025)

There are additional concerns to consider. Generally, AI at the city level is operationalized by a private company, either through procurement or a public-private partnership.²² This sometimes raises ethical questions around private sector access to citizen data. For example, the New York Police Department (NYPD) contracted with a private company to mine and analyze citizen data such as arrest records, parking tickets, and license plates. After the NYPD decided to terminate this contract, the private company refused to turn over the data to the public agency, citing its intellectual property rights to the data analysis it produced throughout the contract term.²³ The company and the NYPD are in an ongoing legal dispute. This is just one example that highlights the need for robust legal frameworks in cities and associated public entities when working with private entities that handle citizen data. The overall complexity of this topic is underscored by a word map which is developed based on the language used by respondents in a global public safety AI survey, where words include discrimination, misuse, safeguards, risk, rapidly, and more, highlighting the degree to which there are reservations from the public on this technology.

Figure 3



Source: Grand View Research

Clearly, cities are well-positioned to lead on responsible AI by focusing on practical implementation, transparency, and building public trust. In tourism, AI is already improving the visitor experience through several practical tools. By paving the way with tangible, high-impact initiatives that pair implementation with strong governance, cities can directly influence the global conversation, showcasing innovation and local leadership to an audience of national governments and international organizations seeking solutions.

The Evolution of Data & AI Policy

Understanding the evolution of data governance provides essential context for how artificial intelligence (AI) intersects with privacy, accountability, and citizens' rights. Modern data protection norms stem from the Fair Information Practices (FIPs) established by the Organisation for Economic Co-operation and Development (OECD) in 1980 and revised in 2013. The FIPs introduced key principles—purpose specification, data quality, use limitation, security safeguards, openness, individual participation, and accountability—that ensure individuals' due process rights over their data while recognizing legitimate state interests in data collection.²⁵ These principles form the foundation of contemporary privacy laws, including the European Union's General Data Protection Regulation (GDPR) and California's state-level privacy framework, both of which emphasize data minimization, purpose limitation, and consent.²⁶ These frameworks collectively oblige public and private entities to collect only necessary data, articulate explicit purposes for doing so, and obtain informed authorization.



As AI technologies expand in capability and influence, they are increasingly governed through the same ethical and legal lenses as data protection—requiring transparency, accountability, and procedural safeguards to ensure responsible use. Foundational privacy principles have evolved into the legal and ethical basis for the global governance of AI.

At the theoretical level, academic institutions have developed models for ethical AI governance. The Rathenau Instituut in the Netherlands, for example, published “Good governance of public sector AI: a combined value framework for good order and a good society”, outlining two complementary ethical concepts for AI in government.²⁷ The first, “good order,” emphasizes responsiveness, effectiveness, and resilience in public institutions, supported by transparency, citizen engagement, political stability, and control of corruption. The second, “good society,” focuses on the moral relationship between governments and citizens—prioritizing autonomy, justice, fairness, dignity, and trust. Together, these frameworks promote AI use that strengthens institutions, enhances accountability, and reinforces social equity and public confidence.

Governments worldwide are translating these academic foundations into operational policy frameworks. The OECD’s 2024 report, “Governing with Artificial Intelligence: Are governments ready?”, identifies three potential benefits of AI in the public sector: greater efficiency and productivity, more inclusive and responsive public services, and enhanced governmental oversight.²⁸ However, it stresses that these outcomes depend on implementing AI systems safely, securely, and transparently. Without strong governance, states risk legal, ethical, and reputational harm.

In response, many governments have issued national guidelines to institutionalize responsible AI practices. Canada’s “Guide on the Use of Generative AI” requires departments to assess and mitigate dataset biases during the design phase to prevent discriminatory outcomes once systems are operational.⁵ Similarly, Australia’s “Artificial Intelligence Ethics Framework” and “Automated Decision-Making Better Practice Guide” provide concrete methodologies for integrating AI ethically across government functions, from design to deployment.²⁹

These ethical and procedural frameworks have, in many cases, informed the development of formal legislative instruments that seek to regulate AI more comprehensively. Moving from voluntary guidance to binding regulation represents an important step in strengthening accountability and public trust.



Regulatory Environment

While ethical frameworks provide guidance, binding regulation remains essential for accountability. The AI regulatory landscape is evolving rapidly across jurisdictions, with Europe leading through the GDPR and the EU AI Act (passed August 2024). Widely viewed as the global standard for AI regulations at this point, the EU AI Act directly addresses privacy and other fundamental rights concerns for its citizens, ensuring that actors across both the public and private sectors are held accountable in their development and deployment of AI programs.³⁰ However, there are concerns around the effectiveness of its implementation from leading experts. While the legislation is robust, enforcing the laws is another question, and one over which there is a level of skepticism as the technology quickly evolves and its deployment scales quickly. This leaves regulatory bodies in a difficult position where they lack the capacity to sufficiently identify and respond to legal infringements.

In the United States, California is widely regarded as the leading state on privacy rights, due in large part to the passing of the California Privacy Rights Act (CPRA), which originally passed in 2020 and took effect in January of 2023. The CPRA guaranteed six key rights for California consumers: The right to know what information a business collects about them, the right to delete personal information collected from them, the right to opt-out of the sharing or sale of personal information, the right to non-discrimination for exercising their data privacy rights, the right to correct inaccurate personal information collected on them by a business, and the right to limit the use and disclosure of information collected on them.³¹ Kevin Werbach, Director of the Wharton Accountable AI, points out that, due to the absence of a federal AI law, many US states are exploring the passage of AI-specific legislation, which highlights the importance of subnational action on this topic.³² Most notably, Colorado passed the Colorado AI Act in 2024, and it is expected to go into effect in February of 2026. This is the state's landmark AI legislation and shares key similarities with the EU AI Act.³³

However, the overwhelming sentiment among AI community experts is that governance is lagging behind implementation, as governments and regulatory bodies struggle to effectively pass legislation that both protects consumers and does not stifle innovation in a sector that has the potential to transform economies. While the EU AI Act has been lauded internationally, there are concerns that it may hinder Europe's ability to compete with the US, China, and other major economies in the AI race, potentially causing the bloc to miss out on billions of dollars in GDP growth.³⁴ Going forward, how governments decide to regulate AI will have major implications not just for consumers and their rights, but also for their own economies, as nations compete for foreign direct investment in data centers, energy projects, and other adjacent technologies and infrastructure that are fueling the growth of artificial intelligence as a sector.



The effectiveness of these legislative and governance frameworks is already being tested in practical and high-risk areas of application. One of the most prominent examples lies within law enforcement and public safety, where AI-driven systems are being increasingly deployed to prevent and respond to crime. There has been a high level of adoption of artificial intelligence within the policing and public safety sphere, as governments seek to reduce crime rates, detain wanted persons, and deter severe threats.³⁵ This raises critical questions about whether these new forms of policing are respecting the Fair Information Principles (FIPs) and the legislation derived from them across jurisdictions worldwide. Predictive policing systems, which analyze data to anticipate where and when crimes may occur and who might be involved, exemplify these challenges.

Within the European Union (EU), this topic has gained attention from leading academics in the space. For example, published in the *AI & Ethics* journal, “Ensuring fundamental rights compliance and trustworthiness of law enforcement AI systems: the ALIGNER Fundamental Rights Impact Assessment”, highlights the EU’s Charter of Fundamental Rights, and the tensions that exist between law enforcement AI and this set of guaranteed rights for all EU citizens. Specifically, the authors cite the following four rights as most relevant to this topic: the Presumption of innocence and right to an effective remedy and to a fair trial, the right to equality and non-discrimination, the freedom of expression and information, the right to respect for private life, and the right to protection of personal data. The paper proposes a Fundamental Rights Impact Assessment tool that can be directly integrated with the EU’s AI governance policies. This tool enables the assessment of high-risk AI systems used by law enforcement agencies, identifies potential fundamental rights violations before AI systems are operationalized, and thereby mitigates potential harm to citizens and society more broadly. This is one example of the concerns around deployment of AI by law enforcement, the clash between AI and guaranteed fundamental rights in places such as the EU, and the need to develop risk-mitigation tools that assess and manage threats to citizen rights and privacy.³⁶

In sum, despite the proliferation of frameworks and legislative action, the pace of innovation continues to challenge regulators’ capacity to safeguard citizens’ rights while enabling technological progress. The next frontier of AI governance will depend on whether governments can build adaptive systems that evolve in parallel with the technology itself.



III. Surveillance Technologies and Alert Systems

Video surveillance equipped with computer vision represents the primary technological infrastructure for AI-powered tourism safety. Modern systems integrate hardware, analytics, and sensor networks to create comprehensive security ecosystems.

Destinations deploy varied camera configurations based on security requirements. Dome cameras are common in indoor and outdoor public settings including transportation hubs, government buildings, and civic centers, offering a discreet profile and vandal-resistant design. Pan-tilt-zoom (PTZ) cameras cover large spaces like public squares and event venues, while fixed cameras monitor critical points such as entrances, checkpoints, and perimeters.³⁷ Specialized equipment includes thermal imaging for low-light monitoring, license plate recognition cameras at parking facilities, and acoustic sensors that detect anomalous sounds, such as gunshots or breaking glass.

AI-embedded cameras process video at the edge, automatically detecting typical objects (people, vehicles, bags), behaviors (loitering, crowding, trespassing, falling), and anomalies, facilitating live alerts for rapid response. AI-powered analytics trains computers to monitor surveillance cameras, detecting abandoned luggage and identifying by whom, recognizing individuals on no-fly lists through facial identification, identifying when people remain within specific areas longer than defined times, and triggering alarms when passengers enter unauthorized zones. AI algorithms monitor entire airport areas through multiple cameras 24/7, identifying and tracking suspicious objects or persons, with immediate alerts of access violations and odd behavior sent to staff.³⁸ Behavioral analytics examines movement patterns such as dwell time, trajectories, and interactions to flag security concerns before incidents escalate by learning baseline “normal” patterns and recognizing anomalies.³⁹

Once a risk is identified, detection systems initiate pre-programmed notification processes to the central software platform for immediate action.⁴⁰ Modern platforms employ tiered alert architectures to ensure timely intervention while minimizing false alarms. Systems automatically classify alerts by severity: critical threats (weapon detection, high-security intrusions, watchlist matches) trigger immediate notifications with video footage, precise location data, and recommended response protocols; medium-priority alerts (prolonged loitering, crowd density issues) queue for operator review; low-priority notifications (minor infractions, maintenance issues) log for routine review and trend analysis.



Integrating mass notification with video surveillance and a centralized software platform provides numerous benefits, including improved situational awareness, faster response times, targeted communications, and improved coordination among agencies. Security Operations Centers (SOCs) receive alerts through Video Management Systems (VMS) consolidating feeds from hundreds or thousands of cameras, enabling operators to track individuals across multiple views, coordinate response teams, and document incidents. In airports, surveillance cameras are strategically placed to cover critical areas, including entrances, exits, ticket counters, baggage claim areas, gates, retail tenants, and restricted areas.

Secure mobile applications enable response teams to access remote video, receive navigation assistance, and gather real-time intelligence. Advanced systems incorporate feedback loops where operators mark alerts as true positives, false positives, or ambiguous, enabling machine learning algorithms to refine detection models and reduce alert fatigue.

Public Transparency and Privacy Requirements

Privacy regulations across jurisdictions mandate transparency when individuals are subject to automated monitoring. Beyond legal compliance, transparency builds public trust and demonstrates responsible governance.

In the United States, many state laws and local ordinances require commercial properties and public-facing spaces to post notices at entrances and monitored areas, typically with signs stating “24-Hour Video Surveillance” or “Security Cameras in Use,” along with contact details and brief privacy notices explaining the purpose. Sign placement matters, requiring posting near main entrances, gates, and parking lots at eye level and in well-lit areas.⁴¹ Under GDPR, clear signage must detail the purpose of data collection, the data controller, and contact details of the Data Protection Officer.⁴² Signage should be clearly visible and readable, displaying details about the organization operating the system, its intended purpose, and contact information for queries. Many jurisdictions governed by GDPR in Europe or CCPA in California mandate informing the public about surveillance through clear signage.

Signage serves multiple purposes: it ensures legal compliance, deters crime, as studies show that potential intruders are less likely to target properties advertising security monitoring, and provides legal defensibility by demonstrating reasonable steps to notify individuals.



Beyond physical signage, destinations adopt digital mechanisms including detailed privacy policies on websites explaining what data is collected and retained, real-time notifications through visitor apps when entering monitored zones, QR codes linking to comprehensive privacy information in multiple languages, and surveillance registries, which are publicly accessible databases documenting locations, types, and purposes of deployed technologies. Barcelona's municipal algorithm registry and Amsterdam's public AI register exemplify this approach.

Under GDPR, individuals have the right to access personal data held about them, including CCTV footage, with organizations required to comply with subject access requests within one month. Video surveillance in the EU is considered personal data under GDPR if recordings can be used to identify an individual. AI systems employing facial recognition trigger heightened protections requiring stronger legal justifications. GDPR's grounds for CCTV include the legitimate interests of employers such as ensuring health and safety, which must always be balanced against privacy concerns. Cameras should not be installed in private spaces where individuals expect reasonable privacy, such as bathrooms, changing rooms, and locker rooms.⁴³

Secure access control is essential, with access restricted to authorized personnel, including management, security staff, and individuals whose job duties require it. Storing surveillance footage longer than necessary increases the risk of unauthorized access, data breaches, or misuse, requiring clear retention policies that ensure businesses store footage only for the minimum period required. Clear signage, publicly disclosed policies, and opt-in mechanisms (where feasible) go a long way in respecting privacy, with privacy laws like GDPR requiring organizations to redact personally identifiable information before sharing or storing footage.⁴⁴

Balancing safety and privacy in airports and tourism destinations is a delicate undertaking, requiring surveillance to be implemented with care. The intersection of AI capability, security necessity, and privacy protection represents a defining challenge for tourism destinations. Cities that navigate this terrain successfully will distinguish themselves through both advanced technological deployment and sophisticated governance frameworks that create safe environments for visitors and residents while respecting privacy rights. Effective governance requires ongoing engagement with privacy advocates, technology vendors, tourism representatives, and residents and visitors whose safety and privacy are at stake.



IV. Cities at the Frontier of AI Tourism Safety

Cities are emerging as critical testing grounds for the responsible and transparent deployment of AI. Municipal governments sit at the intersection of policy and practice, where the effects of AI are most directly experienced by citizens and visitors alike.

The role of the city within AI governance and implementation has gained significant traction within academia, as Harvard University, Cornell University, University of Montreal, and other top research institutions globally research and publish on this topic. For example, Harvard Kennedy School Professor and former mayor of Indianapolis, Stephen Goldsmith, authored a paper titled “AI and the Transformation of Accountability and Discretion in Urban Governance”, which focuses on how AI is transforming governance at the municipal level. The paper lays out five guiding principles for urban governance of AI: a focus on equitable AI deployment to ensure that AI does not widen digital inequality amongst citizens, adapting administrative frameworks at the municipal level to encourage AI adoption and cross-department collaboration, robust data governance policies and procedures, proactive human oversight and accountability, and citizen engagement in AI oversight.⁴⁵

A leading scholar focused on municipal AI from the University of Montreal published “Urban AI Governance Must Embed Legal Reasonableness for Democratic and Sustainable Cities”, which applies the “reasonable person standard”, an Anglo-American legal concept originally developed to assess conduct in negligence cases, but over time expanded to assess if actions taken by the government sufficiently balance competing demands and interests (Mukjani, 2025). A core argument of the paper is that in the absence of clear rules or governance frameworks, municipalities should base their decisions on the deployment of AI in accordance with what a “reasonable person” would consider fair in each context.⁴⁶ The researcher further argues that the reasonable person standard is part of a broader need to include citizens in decision-making around municipal AI. Without an understanding of citizens’ perspectives on urban AI deployment and governance, Mukjani argues that cities cannot effectively and justly serve the needs of their citizens, and risk adopting an approach that serves the government’s interests at the expense of the citizens, fomenting distrust, and worsening citizen-city relations over the long term.⁴⁷

Building on these ideas of fairness and participatory governance, the inclusive city concept extends these same principles to encompass both residents and temporary visitors. It underscores the importance of equal treatment, transparency, and respect for individual rights in digital governance at the local level.



According to the “Inclusive City” concept, permanent and temporary residents are granted the same rights. This is a critical consideration in the context of the AI and privacy rights debate, as international tourists can, in many cases, fall into a legal gray area. The inclusive city concept’s interpretation of temporary resident rights, which includes that of tourists, implies that any digital and privacy rights granted to citizens should be granted to tourists as well. National and local governments clearly outlining where foreigners fall within their legal frameworks, particularly as concerns around privacy continue to mount, can be a key step forward in building trust with the international community and encouraging tourism.⁴⁸

As a general best practice, in line with leading global regulatory frameworks such as the EU’s GDPR and AI Act, as well as the California Privacy Rights Act, and the inclusive city ideal, national and subnational governments should strive to afford the same digital rights to permanent residents and visitors. This would not only enhance confidence in the tourist experience and establish a greater level of trust between the government and visitors but would also be a way through which governments can align themselves with ethical AI principles. These principles provide a foundation for understanding how cities must navigate the intersection of public safety, data protection, and visitor trust. They also set the stage for how AI can be responsibly integrated into the tourism ecosystem, where maintaining both security and comfort is paramount.

Beyond traditional public safety concerns, tourism introduces additional challenges for cities, particularly in managing safety during major events, international gatherings, and the use of public spaces. Large-scale events attract crowds that require careful monitoring, international visitors may navigate unfamiliar legal frameworks, and public spaces must strike a balance between accessibility and security. These factors make it essential for cities not only to maintain actual safety but also to manage the perception of safety for residents and tourists alike.

In addition to everyday safety concerns, major international events intensify the challenges of monitoring and crisis management. Effective coordination between government authorities, technology providers, and private sector participants becomes critical. Cities are also reconsidering how public security is visible in tourist areas. Highly armed police presence can sometimes make visitors uneasy, so some cities rely on less intrusive but more efficient monitoring strategies. Dedicated tourism police units in countries such as Malaysia, Turkey, Dubai, and Colombia help maintain order, provide assistance, and increase traveler confidence while reducing crime.



Major venues can also be core actors in the deployment of public safety AI, with Real Madrid's Santiago Bernabéu Stadium being a key example. This venue hosts millions of visitors annually and partners with leading international technology companies to design and deploy AI-enabled systems that enhance the stadium's safety.⁴⁹

Another example is Colombia's "Ojos en Todas Partes" or Eyes Everywhere program. This initiative allows citizens and tourists to report suspicious or criminal behavior through technology-based tools. It also helps ensure accountability for private sector actors, such as hotels and restaurants, who may be complicit in illegal activities. Similar programs throughout Latin America and Southeast Asia have strengthened coordination between public authorities and private stakeholders, improving overall safety and trust for visitors.⁵⁰

These examples show how cities are combining technology and governance strategies to create safer tourism environments. The key challenge is to apply these tools responsibly, protecting visitors while maintaining privacy, comfort, and trust.



V. AI in Practice: City Implementation

Against this evolving regulatory backdrop, cities worldwide are deploying AI across multiple domains of tourism safety. The following section examines real-world applications, demonstrating how destinations are navigating the complex terrain between innovation and compliance.

In the realm of public safety and law enforcement, municipalities increasingly utilize AI for predictive policing through hotspot analysis, real-time surveillance systems, suspicious behavior detection algorithms, and facial recognition technologies to locate wanted or missing persons. Spatial monitoring tools analyze satellite imagery, camera feeds, and mapping data to identify encampments, assess public space usage during high-risk events, and enable more efficient allocation of security resources in areas with concentrated visitor activity.⁵¹

Building on these surveillance capabilities, transportation infrastructure represents another critical domain for AI integration, where technology enhances mobility while improving overall urban safety. Intelligent traffic management systems, exemplified by solutions from providers like Google⁵² leverage AI to optimize traffic flow, reduce congestion, and minimize accident risks in areas with high tourist volumes. Beyond vehicular traffic, cities are augmenting pedestrian and cyclist safety through AI-powered monitoring systems that detect potential hazards and adjust signal timing to protect vulnerable road users. Predictive maintenance algorithms analyze infrastructure conditions to identify road deterioration before it becomes dangerous, while risk mapping programs help cities prioritize interventions. Public transit systems benefit similarly, with AI optimizing routes and schedules based on real-time occupancy patterns, improving service reliability for all riders.

AI applications are transforming emergency management systems, enabling faster detection and more effective responses to natural disasters and infrastructure failures. In water management, integrated systems utilize real-time sensor data to monitor water levels and generate flash flood predictions and early warnings. Meanwhile, satellite and drone imaging assist in mapping flood extent and coordinating evacuation efforts, particularly in coastal tourist destinations vulnerable to storm surges.⁵² Seismic monitoring represents another area of significant advancement, with technology companies such as SeismicAI demonstrating AI's capacity to detect earthquake precursors and issue rapid alerts that can save lives.⁵³ Similarly, wildfire monitoring systems enhanced by AI analyze weather patterns, vegetation conditions, and historical fire data to predict fire behavior and spread with greater accuracy, enabling timely evacuations in vulnerable tourist areas and residential zones.



Aviation security exemplifies the mature integration of AI in tourism safety infrastructure, with airports worldwide adopting sophisticated technologies that balance security imperatives with passenger experience. Facial recognition systems have become a standard feature at international airports, streamlining identity verification and customs processes while enhancing border security against potential threats. In an era of heightened vigilance, video surveillance systems integrated with AI behavioral analysis algorithms detect suspicious activities and individuals, enabling security personnel to respond more rapidly to emerging risks. Beyond threat detection, AI contributes to operational efficiency and passenger satisfaction through crowd management systems that optimize passenger flow through security checkpoints, reducing wait times while maintaining thorough screening protocols. Advanced baggage scanning systems powered by AI can identify potential threats more accurately and efficiently than traditional methods, simultaneously enhancing security while accelerating the screening process, a dual benefit particularly valuable at high-volume international gateways serving global tourism markets.

Advancing responsible AI implementation in tourism safety requires active collaboration between municipal governments and private sector technology providers. Industry leaders emphasize that public-private partnerships are essential for scaling safe and effective solutions. Jon Berroya, Director of Public Policy at Google, highlights the value of open-source data in helping cities address challenges such as road safety and air quality, noting both the efficiency gains for municipal governments and the importance of initiating these conversations at the subnational level. Edward Parkinson, President of Public Sector at RapidSOS, an intelligent safety platform connecting data from over 600 million devices and buildings to emergency responders worldwide, stresses the need for robust data-sharing channels across public safety agencies. RapidSOS's collaboration with Uber in Rio de Janeiro to improve security for drivers and riders exemplifies how private sector partnerships can expand AI's impact in urban safety contexts. These examples demonstrate that integrating private sector expertise can accelerate innovation while ensuring solutions remain ethical, equitable, and aligned with public interests.

While these applications demonstrate AI's substantial contributions to urban and tourism safety, current implementations reveal a significant gap in scope and focus. The vast majority of deployments focus on physical security, including crime prevention, transportation management, and disaster response, while the digital and psychological dimensions of safety remain comparatively underserved. Few cities have implemented comprehensive tools to strengthen cybersecurity infrastructure, protect visitor data privacy, or detect online threats that could undermine tourist confidence.



Similarly, applications that enhance psychological safety, such as promoting transparent communication, fostering social inclusion, or building public trust, remain largely underdeveloped. This persistent emphasis on physical security highlights the need for more comprehensive frameworks that systematically integrate digital and psychological safety considerations into smart city strategies, ensuring that technology serves the full spectrum of visitor and resident well-being.

The Cities Coalition for Digital Rights, an initiative originally launched by Amsterdam, New York, and Barcelona, represents one of the most concerted efforts by cities worldwide to define a people-centered approach to digital governance. Under its third mission, “Promote the use of digital technologies, data and AI for good,” the Coalition recently released its AI Governance Maturity Survey, a first-of-its-kind global assessment of how cities are managing artificial intelligence at the municipal level. Organized by Toronto and New York, the survey gathered insights from cities across the Americas, Europe, and Asia, providing a comprehensive snapshot of the current state of AI governance in urban environments.⁵⁵

The findings reveal a rapidly evolving but uneven landscape. Over half (52%) of participating cities reported that they are already using AI in some capacity, with an additional 32% planning to do so in the near future. The vast majority (88%) identified improving service delivery and quality of life as their primary motivation for AI adoption, emphasizing a pragmatic, outcome-oriented approach rather than purely experimental innovation. However, the results also highlight a critical gap between intention and governance. While 88% of cities rated ethics as “very or absolutely important,” only 31% have established a formal ethics review process. Cities are prioritizing implementation and experimentation over regulation, as 47% reported prioritizing pilots, while only 12% identified AI policy creation as a top priority.⁵⁶ Additionally, according to 451 Research's Voice of the Enterprise survey, 50% of government respondents identified ensuring public safety as the primary driver for their smart city initiatives, highlighting the key role of public safety in both AI implementation and deployment.

Notably, 82% of respondents believe that local governments should play a direct role in regulating AI, reinforcing the argument that municipal-level governance must evolve alongside national and international frameworks. In developing their own local policies, many cities referenced established international standards such as the EU AI Act, the OECD AI Principles, the NIST Risk Management Framework, and various national executive orders. Despite these positive steps, uncertainty remains high amongst city officials. When asked whether AI is headed in a helpful or harmful direction, a majority (54%) of respondents said it was “too soon to know.” This uncertainty underscores the complex balance cities must strike between innovation, ethical responsibility, and public trust.⁵⁷



Case Studies

These case studies examine five cities demonstrating distinct approaches to AI deployment in tourism safety, each navigating the tension between technological capability and governance responsibility.

The selected cities are London, Barcelona, Helsinki, Singapore, and Miami, representing diverse geographies, regulatory contexts, and strategic priorities, yet sharing common commitments to responsible innovation. London exemplifies the integration of AI across transit safety and policing, while grappling with public concerns over facial recognition technology. Barcelona exemplifies governance-first AI adoption through structured ethical oversight mechanisms. Helsinki demonstrates radical transparency via public AI registries and international collaboration. Singapore showcases strategic public-private partnerships supporting both mega-events and everyday visitor experiences. Miami pioneers workforce development, preparing law enforcement for AI-assisted policing in a high-tourism environment.

Together, these cases illuminate how cities can leverage AI to address the three key dimensions of tourism safety: physical security through enhanced detection and response, digital protection through secure data practices, and psychological assurance through transparent governance. Each case offers replicable strategies while highlighting context-specific challenges that cities must navigate based on their unique legal frameworks, public expectations, and tourism profiles.

London: AI for Transit Safety and Enhanced Policing Systems

London exemplifies the operational gains AI can deliver in high-volume transit environments, while simultaneously highlighting the governance tensions that emerge when surveillance technologies expand without sufficient public consensus. Transport for London's (TfL) AI-powered platform safety system deploys smart video monitoring to detect anomalies on underground platforms, distinguishing between regular train activity and dangerous objects on tracks to trigger rapid staff intervention. Deployed at stations such as Custom House following a recent fatal accident, the system addresses urgent physical safety needs in a transit network serving millions of daily users, including substantial tourist traffic.⁵⁸ This initiative integrates with TfL's broader Data for London Library, an open data platform connecting datasets from multiple public agencies to enhance decision-making across safety, mobility, and health services. The platform illustrates how AI can strengthen physical safety infrastructure while supporting broader urban intelligence systems.



However, London's deployment of facial recognition technologies through mobile surveillance vans in high-footfall areas has generated significant public controversy. While Metropolitan Police officials defend the technology as effective and bias-free for identifying suspects in serious crimes, civil liberties organizations cite the need for more robust legal frameworks and transparency mechanisms. The technology's deployment in areas frequented by tourists raises questions about visitor privacy rights and whether travelers receive adequate notice of biometric surveillance. A formal public consultation now underway seeks to address these concerns and explore regulatory options.⁵⁹

London's experience demonstrates that technological capability alone cannot ensure successful AI deployment in tourism contexts. Visitor confidence depends not only on effective security measures but also on perceived legitimacy of surveillance practices. Cities must balance operational efficiency gains against public expectations for oversight, transparency, and proportionality, particularly when serving diverse international populations with varying privacy norms and legal protections.

Barcelona: Leading on Ethical AI Governance

Barcelona demonstrates how cities can establish comprehensive ethical frameworks before scaling AI deployment, prioritizing accountability over speed to market. The city's municipal strategy on algorithms and data outlines clear principles rooted in transparency and privacy oversight, explicitly rejecting fully automated decision-making in favor of recommendation engines that preserve human judgment in consequential decisions. This governance-first approach addresses all three dimensions of tourism safety: physical security through responsible surveillance deployment, digital protection through data minimization requirements, and psychological safety through transparent communication about algorithmic systems.

To institutionalize oversight, Barcelona established an External Advisory Council on AI, composed of independent experts who evaluate the risks and impacts of high-stakes algorithms before deployment, alongside an internal Commission on Ethical Urban AI that brings together representatives from across city departments to ensure consistent implementation. A dedicated internal protocol guides ethical design, procurement, and dismantling of AI systems based on assessed risk levels. Barcelona has also contributed to the Algorithmic Transparency Standard, a European initiative promoting open, standardized registries of AI tools used in public administration.⁶⁰ For tourism safety specifically, Barcelona's framework influences how the city manages crowd control during peak seasons, processes visitor data at municipal facilities, and deploys surveillance in high-traffic areas, such as Las Ramblas and the Gothic Quarter.



Rather than maximizing data collection, the city's data minimization principle limits surveillance to what is necessary and proportionate, addressing visitor privacy concerns while maintaining security capabilities. By requiring human oversight for consequential algorithmic decisions, Barcelona ensures that visitors encountering municipal AI systems, whether through parking enforcement, facility access control, or emergency response, interact with accountable governance structures rather than opaque automation.

Barcelona's model demonstrates that ethical governance frameworks can facilitate innovation rather than impede it, channeling it toward socially acceptable and legally compliant applications. For cities seeking to build trust with both residents and international visitors, Barcelona's structured approach offers replicable institutional mechanisms that balance multiple stakeholder interests.⁶¹

Helsinki: Transparency and International Collaboration

Helsinki has pioneered radical transparency in municipal AI governance through the Helsinki AI Register, a publicly accessible platform allowing residents and visitors to view, understand, and provide feedback on the city's algorithmic systems. The register details what each AI tool does, what data it uses, how decisions are made, and who is accountable for outcomes. For international visitors navigating urban services, this transparency model directly addresses psychological safety by making algorithmic governance visible and contestable rather than hidden and presumptive.

The register currently documents AI applications across multiple domains relevant to tourism safety, including mobility management systems that optimize traffic flows in high-tourist areas, facility access controls at public buildings and attractions, and emergency response coordination tools. By providing this information in accessible formats, Helsinki enables visitors to understand how their data is used and what protections are in place, building confidence that surveillance serves legitimate security purposes rather than excessive monitoring.⁶²

Helsinki's approach extends beyond domestic transparency to active international collaboration on AI governance standards. The city participates in EU-funded crossborder partnerships through its innovation agency, Forum Virium, which facilitates knowledge exchange on responsible AI deployment. These collaborations inform Helsinki's evolving practices and contribute to emerging European standards for municipal AI governance, yielding insights applicable across diverse urban contexts, including tourist-heavy cities managing complex visitor flows and digital services.⁶³



The city's commitment to openness establishes accountability mechanisms that operate across jurisdictions, a particularly valuable feature for tourism destinations serving international populations with diverse expectations regarding privacy and data protection. When visitors from GDPR-governed countries, CCPA-regulated California, or jurisdictions with weaker privacy protections all interact with Helsinki's systems, the register provides common ground for understanding what protections apply and how to exercise rights.

Singapore: AI-Enhanced Tourism Safety

Singapore illustrates how strategic public-private partnerships can advance AI deployment across tourism safety applications while maintaining centralized governance oversight. The Singapore Tourism Board's formal partnership with OpenAI to test generative AI applications for destination marketing, experience customization, and productivity enhancement reflects the city-state's Tourism 2040 strategy, which positions digital transformation as essential to sustained sector growth. This governance structure ensures that innovation serves clearly defined public objectives rather than merely commercial interests.⁶⁴

At large-scale events like the Marina Bay Countdown, the Singapore Police Force deploys AI-equipped drones conducting real-time crowd monitoring through heat mapping and panoramic imaging. These systems identify congested zones, predict crowd flow patterns, and broadcast safety messages through onboard speakers, enabling proactive intervention before dangerous conditions emerge. Ground-level LED signage supplements aerial monitoring by directing pedestrian flows during peak hours, creating an integrated physical safety infrastructure that combines multiple technological layers with human oversight.⁶⁵

Changi Airport exemplifies Singapore's approach to comprehensive AI integration across the visitor journey. Automated baggage scanning systems accelerate security processing while maintaining detection accuracy. Facial recognition enables seamless, passport-free clearance for registered travelers, and predictive analytics optimize facility operations, from restroom cleaning schedules to retail staffing levels. These applications address all three safety dimensions: physical security through enhanced threat detection, digital protection through secure biometric processing, and psychological assurance through operational efficiency that minimizes visitor stress and confusion. Critically, Singapore's AI deployment operates within clear governance parameters established by national frameworks including the Model AI Governance Framework and the Personal Data Protection Act.



These structures require organizations deploying AI to conduct impact assessments, maintain human oversight for consequential decisions, and provide transparency about algorithmic operations. For tourism applications, this means visitors benefit from AI-enhanced services while retaining legal protections and recourse mechanisms if systems malfunction or produce discriminatory outcomes.⁶⁶

Singapore's model demonstrates that ambitious AI deployment and robust governance can coexist when clear frameworks precede technological rollout. For cities seeking to leverage AI as a competitive advantage in global tourism markets, Singapore provides evidence that responsible governance enhances, rather than constrains, innovation.

Miami: Training AI-Enabled Public Safety Officers

Miami exemplifies how AI deployment in tourism safety depends not only on technological infrastructure but also on workforce readiness. In 2025, Miami Dade College's School of Justice, Public Safety and Law Studies became the first U.S. police academy to train recruits using an AI-powered assistant. Developed by law enforcement technology company TRULEO, the tool enhances policing capabilities through body-worn camera analysis, voice-dictated report generation, real-time policy guidance, and virtual dispatch support, preparing officers to protect both residents and the city's millions of annual visitors.

The system now forms part of the Florida Law Enforcement Academy curriculum, training officers from over 35 police departments and producing thousands of graduates annually. This adoption represents more than technological modernization; it reflects recognition that AI deployment succeeds only when human operators understand both capabilities and limitations of algorithmic tools. Training emphasizes not merely how to use AI assistants but also when to override AI recommendations, how to detect potential algorithmic errors, and what legal and ethical constraints govern AI-assisted policing.⁶⁷

For Miami, a major international tourism destination that has faced significant crime challenges affecting visitor perceptions, this workforce investment addresses critical needs. Tourist areas, including South Beach, the Port of Miami, and the Design District, require security approaches that balance protection with the welcoming atmosphere essential to tourism economies. AI-assisted policing promises faster response times, better resource allocation, and more consistent documentation of incidents involving visitors, potentially improving both actual security and perceived safety.⁶⁸



However, Miami's approach also highlights unresolved questions about AI in policing that particularly affect tourism contexts, such as how body camera analysis will handle interactions with international visitors speaking multiple languages, what transparency obligations exist when AI assists in encounters with tourists who may be unfamiliar with U.S. legal systems, and how can cities ensure AI-assisted policing serves rather than surveils diverse visitor populations. Miami's integration of AI training provides the workforce with the capacity to address these questions, but municipal governance frameworks must evolve alongside technological and training capabilities.

Miami's case demonstrates that technology, governance, and human capital development must advance together. Cities investing heavily in AI infrastructure without corresponding workforce development risk deployment failures, while those training personnel without adequate governance frameworks risk misuse. Miami's balanced approach, integrating AI tools with structured training and growing awareness of governance needs, offers a model for other tourism-dependent cities seeking to modernize public safety without sacrificing accountability.

Comparative Insights

These five cases reveal that no single approach to AI in tourism safety dominates.

London demonstrates that technological sophistication without public consensus generates backlash, undermining legitimacy.

Barcelona shows that comprehensive governance frameworks can channel innovation toward socially acceptable applications.

Helsinki proves that real transparency builds trust across diverse visitor populations with varying privacy expectations.

Singapore exemplifies how strategic public-private partnerships, under centralized oversight, can deliver both innovation and accountability.

Miami highlights that workforce development must parallel technological deployment to ensure responsible operation.

Common across successful implementations are several principles: explicit governance frameworks established before large-scale deployment, transparency mechanisms that make algorithmic operations visible and contestable, protection of all three safety dimensions (physical, digital, and psychological), engagement with multiple stakeholders including privacy advocates and civil society, and continuous evaluation with willingness to adjust or halt problematic deployments. Cities that treat AI as merely a technical challenge, procuring systems without addressing governance, consistently encounter public resistance, legal challenges, and reputational damage that undermine both security effectiveness and tourism competitiveness. Those that balance technological capability with institutional accountability position themselves as leaders in responsible innovation, attracting visitors who value both safety and digital rights.

**Table 1: Comparative Analysis of AI Deployment in Tourism Safety**

City	Primary Focus	Key Innovation	Governance Approach	Tourism Application
London	Transit safety & policing	Platform monitoring systems	Adaptive governance emphasizing transparency and evolving public engagement	High-volume transit networks
Barcelona	Ethical frameworks	Pre-deployment algorithmic review	Proactive, structured oversight	Crowd management in tourist districts
Helsinki	Transparency	Public AI register	Open, collaborative, international	Cross-jurisdictional trust-building
Singapore	Strategic partnerships	Integrated event & airport systems	Centralized national oversight	Mega-events and seamless travel
Miami	Workforce development	AI-assisted police training	Emerging, training-led approach	Visitor-area policing modernization

Urban AI Initiatives

As cities continue to integrate AI into the delivery of public services, international organizations and non-profits are increasingly recognizing the need to launch global initiatives that advance this growing field in an ethical and responsible manner.

For example, the cities of Amsterdam, New York, and Barcelona jointly launched the Cities Coalition for Digital Rights.⁶⁹ One of the stated missions of this coalition is to “promote the use of digital technologies data, and AI for good”. Through research, knowledge sharing, and reporting of best practices, the Cities Coalition for Digital Rights continues to be an influential force, highlighting the important role that international coalitions can play in advancing best practices for cities globally on specific topics – in this case, digital and AI governance.

Importantly, this entity has emerged as a leading voice through in-depth and regularly updated surveys, which directly report on the activities of cities around the world. For example, through this coalition, Toronto and New York jointly led a survey which focused on “AI Governance Maturity”, gauging the extent to which cities are developing and instituting local policies on AI governance.

The Global Observatory of Urban Artificial Intelligence (GOUAI) is another major program in the realm of urban AI and is a joint project of CIDOB (Barcelona Centre for International Affairs), the cities of Barcelona, Amsterdam, and London, and UN-Habitat. The goal of the GOUAI is to “promote ethical artificial intelligence systems in cities”, while ensuring that these systems are “sustainable, fair, accountable, transparent, cyber secure, and safeguard people’s digital rights”. The GOUAI serves as the only comprehensive database of city-level AI programs, with a focus on efforts made on governance, highlighting the global nature of AI adoption and local-level action. The observatory highlights the leading cities that are truly leading the way in ethical AI governance policies, striking a balance between implementation and responsible laws, policies, and protocols.

The “Atlas” below (*Figure 4*), from the Global Observatory of Urban Artificial Intelligence, highlights regional concentrations of AI adoption in urban governance, underscoring both the growing global uptake and the uneven distribution of implementation capacity. The numbers within each circle indicate the count of documented AI initiatives or projects in that approximate region, while the size of the circles reflects their relative scale or maturity. The visualization highlights both the global reach of urban AI adoption and the disparities in implementation capacity across different regions.

Figure 4



Source: Global Observatory of Urban Artificial Intelligence (2025)

There is not yet a global initiative that focuses on the topic of public safety AI for tourist safety. Given the significant complexities associated with protecting tourists, the scale of this growing industry, and the importance of local-level policies in driving it forward, this is a critical and under-explored policy area.



VI. The Way Forward

Tourism destinations worldwide, from historic cities and cultural regions to heritage sites and coastal areas, face unprecedented challenges as infrastructure originally designed for resident populations now accommodates mass tourism flows. This shift has created cascading pressures that strain local resources and test community resilience. Destinations grapple with overburdened infrastructure, chronic overcrowding, gentrification that displaces residents, mounting safety concerns, and significant environmental impacts that threaten the very assets that attract visitors. These challenges are not unique to any single location; destinations across the globe confront these common pressures in isolation, often lacking platforms for systematic collaboration and knowledge exchange that could accelerate solutions.

AI Tourism Safety 10-Point Policy Roadmap

Drawing on comprehensive research and expert interviews, the ***AI Tourism Safety 10 Point Policy Roadmap*** presented below aims to provide practical guidance for destinations deploying AI in tourism safety contexts. The recommendations address governance structures, legal frameworks, data management, transparency requirements, and stakeholder engagement.

The Policy Roadmap's Phase 1 establishes foundational governance through local AI tailored to tourism contexts, comprehensive legal protections for citizen data when private companies are involved, and unified data libraries that enable cross-departmental collaboration. Phase 2 builds institutional capacity through internal and external advisory boards representing diverse stakeholders, designated leadership coordinating AI implementation across departments, and public AI registers ensuring transparency. Phase 3 operationalizes innovation through ethics sandboxes for controlled experimentation, mandatory AI literacy training for frontline personnel, systematic evaluation of transport infrastructure for AI integration opportunities, and comprehensive analysis of emergency response systems across disaster scenarios.



Phase 1: Foundation & Governance

- 1 Establish AI governance frameworks tailored to tourism and public safety, defining clear approval, oversight, and accountability processes for all AI deployments, filling a critical gap when national, regional, and international frameworks may be insufficient or nonexistent
- 2 Implement comprehensive legal frameworks that safeguard citizen data whenever private companies collect, process, or manage municipal data, which include explicit rules on data ownership, usage rights, retention periods, security standards, and accountability
- 3 Establish unified data libraries to leverage the full extent of a city's data resources, encourage cross-department collaboration, and build the most effective and smart AI systems

Phase 2: Capacity, Transparency & Data Infrastructure

- 4 Develop internal and external advisory boards that include tourism, hospitality, transport, and technology stakeholders to guide responsible AI implementation and governance, ensuring a well-balanced strategy that encourages private sector innovation and public-private collaboration
- 5 Designate a central point of leadership on AI implementation for tourism safety to coordinate across tourism, technology, public safety, and public relations departments
- 6 Maintain a public AI register that transparently lists each municipal AI system, its purpose, data sources, and safeguards

Phase 3: Applied Innovation

- 7 Establish municipal AI ethics sandboxes that allow controlled experimentation with emerging AI systems for tourism safety before citywide rollout
- 8 Implement mandatory AI literacy and digital rights training for police, transport operators, and tourism staff, ensuring informed and ethical system use that protects the rights of both residents and visitors, while equipping dedicated tourism safety units to effectively apply advanced technologies
- 9 Holistically evaluate public and road transport systems, working closely with the private sector to identify opportunities for advanced data gathering, analysis, and management. AI can then be leveraged to optimize traffic flows, enhance public transit efficiency, and improve overall transit measures that protect both residents and tourists
- 10 Thoroughly analyze emergency response systems across a range of potential natural disaster risks, such as flooding, wildfires, earthquakes, and extreme heat to identify areas where AI can more rapidly predict, identify, and notify the public of material risks to people, property, and infrastructure



This 10-Point Policy Roadmap outlines a framework for destinations seeking to leverage AI for enhancing tourism safety while effectively managing the associated ethical, operational, and governance risks. It acknowledges that destinations operate within varying regulatory environments, possess different technical capacities, and serve diverse visitor populations, requiring adaptation to local contexts rather than a uniform application. Implementation will depend on each destination's specific circumstances, priorities, and resources. However, the core principles—establishing governance before deployment, protecting privacy and data rights, ensuring transparency, building institutional capacity, and maintaining continuous evaluation—apply across contexts.

This Policy Roadmap aims to strengthen and expand ongoing discussions about responsible and effective AI deployment in tourism, a critical issue that continues to evolve as technology advances and implementation experience accumulates. As destinations test solutions, share lessons learned, and adapt approaches to emerging challenges, the AI Tourism Safety 10-Point Policy Roadmap should be refined and enhanced through ongoing dialogue with diverse stakeholders to reflect this collective knowledge. By engaging multiple perspectives and remaining responsive to practical implementation experiences, this Policy Roadmap aims to contribute to shaping a future where AI effectively serves tourism safety goals.



Conclusion

Tourism destinations worldwide stand at a critical juncture in shaping visitor safety. The integration of artificial intelligence offers unprecedented opportunities to enhance public safety, improve emergency response, and strengthen traveler confidence through sophisticated detection and rapid coordination capabilities. However, these benefits can only be realized when technological deployment is paired with robust governance frameworks, clear accountability mechanisms, and unwavering commitment to civil rights, transparency, and non-discrimination.

The evidence presented demonstrates that successful AI deployment in tourism safety depends on addressing three interconnected dimensions simultaneously. Physical security protects visitors from direct threats through surveillance, emergency response, and crime prevention. Digital safety safeguards personal data and privacy rights against cyber threats and unauthorized access. Psychological safety builds visitor confidence through transparent communication and governance that demonstrates respect for individual rights.

AI systems address these dimensions through complementary mechanisms: real-time threat detection for physical security, encryption and access controls for digital protection, and public AI registries with transparent communication for psychological assurance. Destinations treating AI as merely a technical procurement challenge consistently encounter public resistance, legal challenges, and reputational damage that undermine both security effectiveness and tourism competitiveness.

The case studies examined —London, Barcelona, Helsinki, Singapore, and Miami— demonstrate that no single approach dominates. Each city has adapted strategies to its unique context and priorities. Common principles emerge across successful implementations. These include establishing explicit governance frameworks before large-scale deployment; creating transparency mechanisms that enable public understanding and oversight; protecting all three safety dimensions rather than prioritizing physical security alone; engaging multiple stakeholders including privacy advocates and civil society; and maintaining continuous evaluation with willingness to adjust or halt problematic deployments. These implementation lessons directly informed the development of this paper's central contribution: The AI Tourism Safety 10-Point Policy Roadmap.

The Policy Roadmap is organized into three phases, corresponding to implementation stages. Phase 1 addresses foundational governance and legal structures, Phase 2 focuses on capacity building, transparency mechanisms, and data infrastructure, and Phase 3 covers applied innovation and continuous evaluation. The recommendations reflect insights from case study analysis, regulatory review, and practitioner experience across diverse destination contexts.



This phased structure recognizes that cities operate under varying regulatory environments, possess different technical capacities, and serve diverse visitor populations. It is not based in rigid standardization but in identifying the essential governance elements—transparency, accountability, stakeholder engagement, privacy protection, and continuous evaluation—that distinguish responsible AI deployment from implementation without adequate safeguards.

Destinations that prioritize robust AI governance position themselves advantageously in an increasingly competitive global tourism market. Tourism represents a significant economic sector globally, with destinations competing for visitors who increasingly value both safety and digital rights. Travelers making destination choices now consider not only traditional safety metrics but also how their data will be protected, whether surveillance practices respect privacy, and whether algorithmic systems operate transparently. Destinations that successfully balance security imperatives with rights protections will attract these discerning travelers, while those deploying technology without adequate safeguards risk competitive disadvantage as reputation concerns spread through social media and travel advisories. In an interconnected world where visitor perceptions shape destination success, governance quality has emerged as a critical market differentiator.

The future of tourism safety will be shaped not by technological sophistication alone but by the governance structures cities establish to direct it. Destinations that adopt comprehensive approaches while adapting guidance to local contexts, regulatory requirements, and stakeholder priorities—can position themselves as leaders in responsible innovation. The Policy Roadmap presented in this paper aims to represent a systematic approach that cities may utilize, modify, or integrate with existing governance initiatives based on their unique circumstances and institutional capacities. Destinations pursuing such structured approaches can demonstrate that security and civil liberties need not be traded against one another but can advance together when technology serves clearly defined public interests within accountable institutional systems. Their success has the potential to validate a fundamental principle: the most competitive destinations in tomorrow's tourism economy will likely be those that protect visitors most comprehensively—physically, digitally, and psychologically—through intelligent integration of advanced technology and exemplary governance.



Bibliography

Ahmed, A., & Kataria, S. (2025, September 16). Nepal's deadly protests hammer tourism sector as arrivals fall 30%. Reuters. <https://www.reuters.com/world/asia-pacific/nepals-deadly-protests-hammer-tourism-sector-arrivals-fall-30-2025-09-15>

Ambury, B. (2018, August 22). Travellers in favour of using AI at airports. Business Traveller. <https://www.businesstraveller.com/business-travel/travellers-in-favour-of-ai-at-airports/>

"Bloomberg Philanthropies Survey Reveals High Mayoral Interest in AI, Low Implementation." Bloomberg Cities, Bloomberg Philanthropies, Oct. 2023, <http://bloombergcities.jhu.edu/news/cities-are-ramping-make-most-generative-ai>.

Brennan Center for Justice. (2025, September 30). Palantir contract dispute exposes NYPD's lack of transparency. Retrieved October 23, 2025, from <https://www.brennancenter.org/our-work/analysis-opinion/palantir-contract-dispute-exposes-nypds-lack-transparency>

Brayne, S. (2020). Predict and surveil: Data, discretion, and the future of policing. Oxford University Press.

California Privacy Protection Agency. (n.d.). California Privacy Rights Act (CPRA) of 2020. <https://cpa.ca.gov/regulations/>

Caseguard. (2024, August 6). Artificial intelligence, video footage, and airport security. <https://caseguard.com/articles/ai-in-airport-video-surveillance/>

5 City of Helsinki. (2022, November 22). The City of Helsinki established principles for the ethical use of data and artificial intelligence. <https://www.hel.fi/en/news/the-city-of-helsinki-established-principles-for-the-ethical-use-of-data-and-artificial-intelligence>

Colorado General Assembly. (2024). Colorado Artificial Intelligence Act, House Bill 231310. <https://leg.colorado.gov/bills/hb23-1310>

Coram AI. (2025, October). Security cameras for public places: Video surveillance and public safety. <https://www.coram.ai/post/security-cameras-for-public-places>

BBC News. (2025, January 17). Transport for London aims to use more AI to boost platform safety. BBC. <https://www.bbc.com/news/articles/cdojgm1nzzo>

European Commission. (2021). Proposal for a regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) (COM/2021/206 final). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206>

37 European Parliament Research Service. (2021). Artificial intelligence: From ethics to policy (EPRS BRI(2021)698792 EN). [https://www.europarl.europa.eu/Reg-Data/etudes/BRIE/2021/698792/EPRS_BRI\(2021\)698792_EN.pdf](https://www.europarl.europa.eu/Reg-Data/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf)

Euromonitor International. (2024). Top 100 city destinations index 2024. As reported in Travel and Tour World. Retrieved October 24, 2025, from <https://www.travelandtourtworld.com/news/article/bangkok-tops-global-tourism-rankings-for-2024-record-32-4-million-visitors-and-innovative-traveller-friendly-policies-elevate-thai-capital-to-unrivaled-global-recognition>



Facit Data Systems. (2025, February 13). CCTV video analytics in airports. <https://facit.ai/insights/airport-cctv-analytics-video-compliance>

Ferguson, A. G. (2017). *The rise of big data policing: Surveillance, race, and the future of law enforcement*. NYU Press.

Florido Benítez, L., Giglio, R., & Campos Soria, J. A. (2025). The role of cybersecurity as a preventive measure in digital tourism and travel: A systematic literature review. *Discover Computing*, 28, Article 28. <https://doi.org/10.1007/s10791-025-09523-3>

Xu, C. (2024). Applications and challenges of artificial intelligence in disaster prevention, reduction, disaster relief, and emergency management. *International Journal of Disaster Risk Science*. Advance online publication. <https://www.sciencedirect.com/science/article/pii/S266659212300121X>

Casaburo, D., & Marsh, I. (2024). Ensuring fundamental rights compliance and trustworthiness of law-enforcement AI systems: The ALIGNER Fundamental Rights Impact Assessment. *AI and Ethics*, 4(4), 1569–1582. <https://link.springer.com/article/10.1007/s43681-024-00560-0>

Goldsmith, S. (2023). AI and the transformation of accountability and discretion in urban governance. Ash Center for Democratic Governance and Innovation, Harvard Kennedy School. <https://ash.harvard.edu/publications/ai-and-transformation-accountability-and-discretion-urban-governance>

Hao, K. (2023). Rethinking privacy in the AI era: Policy provocations for a data-centric world [White paper]. Stanford Institute for Human-Centered Artificial Intelligence. <https://hai.stanford.edu/white-paper-rethinking-privacy-ai-era-policy-provocations-data-centric-world>

The Guardian. (2025, May 24). Police live-facial-recognition cameras England and Wales. <https://www.theguardian.com/technology/2025/may/24/po-lice-live-facial-recognition-cameras-england-and-wales>

Ipsos. (2025, July 25). Travel is booming despite global uncertainty and climate concerns. Retrieved October 23, 2025, from <https://www.ipsos.com/en-tw/travel-booming-despite-global-uncertainty-and-climate-concerns>

Liang, L.-H. (2025, November 3). Metropolitan Police to expand live facial recognition use even amid legal challenge. *Biometric Update*. <https://www.biometricupdate.com/202511/metropolitan-police-to-expand-live-facial-recognition-use-even-amid-legal-challenge>

McLendon, B. S. (2025, May 1). Miami Dade Police Academy adds AI training for future officers. *Miami New Times*. <https://www.miaminewtimes.com/news/miami-dade-police-academy-adds-ai-training-for-future-officers-22997573>

Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. *Big Data & Society*, 3(2), 2053951716679679. <https://doi.org/10.1177/2053951716679679>



49 Mushkani, R. (2025, August 16). Urban AI Governance must embed legal reasonableness for democratic and sustainable cities (arXiv preprint 2508.12174). <https://arxiv.org/abs/2508.12174>

Organisation for Economic Co-operation and Development. (2013). Privacy expert group report on the review of the 1980 OECD Privacy Guidelines. OECD Digital Economy Papers No. 229. <https://doi.org/10.1787/5k3xz5zmj2mx-en>

Organisation for Economic Co-operation and Development. (2024). Governing with artificial intelligence: Are governments ready? (OECD Artificial Intelligence Papers No. 20). OECD Publishing. <https://doi.org/10.1787/26324bc2-en>

Organisation for Economic Co-operation and Development. (2025, June). AI in public service design and delivery: Governing with artificial intelligence. OECD Publishing.

Personal Data Protection Commission (PDPC). (2020, January 21). Model AI Governance Framework – Second Edition. Singapore: PDPC. <https://www.pdpc.gov.sg/help-and-resources/2020/01/model-ai-governance-framework>

Pimloc Ltd. (2025, May 16). Video surveillance in airports: Balancing privacy and security. SecureRedact. <https://www.secureredact.ai/articles/video-surveillance-in-airports>

Scylla Technologies. (2025). How leveraging AI helps optimize safety and security for airports. <https://www.scylla.ai/how-leveraging-ai-helps-optimize-safety-and-security-for-airports/>

Security Magazine. (2025, June 30). Integrating mass notification with video surveillance in airports. <https://www.securitymagazine.com/articles/101730-integrating-mass-notification-with-video-surveillance-in-airports>

Sirix Monitoring. (2025, June 24). 2025 surveillance compliance: What businesses need to know. <https://sirixmonitoring.com/blog/surveillance-compliance-what-businesses-need-to-know/>

Smart Nation Singapore. (2023). Smart Nation and Digital Government Group. <https://www.smartnation.gov.sg/>

Tico Times. (2025, April 22). Costa Rica faces tourism slump despite high season. <https://ticotimes.net/2025/04/22/costa-rica-faces-tourism-slump-despite-high-season>

51 United Nations Human Settlements Programme (UN-Habitat). (2020). Inclusive cities: Enhancing the positive impact of urban migration (FP4). https://unhabitat.org/sites/default/files/2020/01/fp4-inclusive-cities_-_enhancing_the_positive_impact_of_urban_migration_v261119.pdf

United Nations Interregional Crime and Justice Research Institute. (2024, November). “Not just another tool”: Public perceptions of AI in law enforcement [PDF]. <https://unicri.org/sites/default/files/2024-11/Public-Perceptions-Police-Use-Artificial-Intelligence.pdf>

World Health Organization. (2025, March 19). Urban health [Fact sheet]. <https://www.who.int/news-room/fact-sheets/detail/urban-health>

World Travel & Tourism Council. (2024). Travel & tourism economic impact research (EIR). <https://wttc.org/research/economic-impact>



- 1** Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. *Big Data & Society*, 3(2), 2053951716679679. <https://doi.org/10.1177/2053951716679679>
- 2** “Bloomberg Philanthropies Survey Reveals High Mayoral Interest in AI, Low Implementation”; Bloomberg Cities, Bloomberg Philanthropies, Oct. 2023, bloombergcities.jhu.edu/news/cities-are-ramping-make-most-generative-ai.
- 3** European Commission. (2021). Proposal for a regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX-3A52021PC0206>
- 4** Liang, L.-H. (2025, November 3). Metropolitan Police to expand live facial recognition use even amid legal challenge. *Biometric Update*. https://www.biometricupdate.com/202511/metropolitan-police-to-expand-live-facial-recognition-use-even-amid-legal-challenge?utm_source=chatgpt.com
- 5** City of Helsinki. (2021). AI strategy 2021–2025. <https://www.hel.fi/static/liitteet/2019-2023/Tekoaly-strategia-2021-2025-en.pdf>
- 6** Smart Nation Singapore. (2023). Smart Nation and Digital Government Group. <https://www.smartnation.gov.sg/>
- 7** McLendon, B. S. (2025, May 1). MiamiDade Police Academy adds AI training for future officers. *Miami New Times*. <https://www.miaminewtimes.com/news/miami-dade-police-academy-adds-ai-training-for-future-officers-22997573>
- 8** World Travel & Tourism Council. (2024). Travel & Tourism Economic Impact Research (EIR). Retrieved October 23, 2025, from https://wtcc.org/research/economic-impact?utm_source=chatgpt.com
- 9** World Travel & Tourism Council. (2024). Travel & Tourism Economic Impact Research (EIR). Retrieved October 23, 2025, from https://wtcc.org/research/economic-impact?utm_source=chatgpt.com
- 10** Ipsos. (2025, July 25). Travel is booming despite global uncertainty and climate concerns. Retrieved October 23, 2025, from https://www.ipsos.com/en-tw/travel-booming-despite-global-uncertainty-and-climate-concerns?utm_source=chatgpt.com
- 11** Ipsos. (2025, July 25). Travel is booming despite global uncertainty and climate concerns. Retrieved October 23, 2025, from https://www.ipsos.com/en-tw/travel-booming-despite-global-uncertainty-and-climate-concerns?utm_source=chatgpt.com
- 12** Ahmed, A., & Kataria, S. (2025, September 16). Nepal's deadly protests hammer tourism sector as arrivals fall 30%. *Reuters*. Retrieved October 23, 2025, from https://www.reuters.com/world/asia-pacific/nepals-deadly-protests-hammer-tourism-sector-arrivals-fall-30-2025-09-15/?utm_source=chatgpt.com
- 13** Tico Times. (2025, April 22). Costa Rica faces tourism slump despite high season. Retrieved October 23, 2025, from https://ticotimes.net/2025/04/22/costa-rica-faces-tourism-slump-despite-high-season?utm_source=chatgpt.com
- 14** Florido Benítez, L., Giglio, R., & Campos Soria, J. A. (2025). The role of cybersecurity as a preventive measure in digital tourism and travel: A systematic literature review. *Discover Computing*, 28, Article 28. <https://doi.org/10.1007/s10791-025-09523-3>
- 15** World Health Organization. (2025, March 19). Urban health [Fact sheet]. Retrieved October 23, 2025, from https://www.who.int/news-room/fact-sheets/detail/urban-health?utm_source=chatgpt.com



- 16** Euromonitor International. (2024). Top 100 City Destinations Index 2024. As reported in Travel and Tour World. Retrieved October 24, 2025, from https://www.travelandtourworld.com/news/article/bangkok-tops-global-tourism-rankings-for-2024-record-32-4-million-visitors-and-innovative-traveller-friendly-policies-elevate-thai-capital-to-unrivalled-global-recognition?utm_source=chatgpt.com
- 17** Ipsos. (2025, July 25). Travel is booming despite global uncertainty and climate concerns. Retrieved October 23, 2025, from <https://www.ipsos.com/en-tw/travel-booming-despite-global-uncertainty-and-climate-concerns>
- 18** R. Mushkani, personal communication, September 30, 2025
- 19** United Nations Interregional Crime and Justice Research Institute. (2024, November). "Not Just Another Tool": Public perceptions of AI in law enforcement [PDF]. Retrieved October 23, 2025, from <https://unicri.org/sites/default/files/2024-11/Public-Perceptions-Police-Use-Artificial-Intelligence.pdf>
- 20** United Nations Interregional Crime and Justice Research Institute. (2024, November). "Not Just Another Tool": Public perceptions of AI in law enforcement [PDF]. Retrieved October 23, 2025, from <https://unicri.org/sites/default/files/2024-11/Public-Perceptions-Police-Use-Artificial-Intelligence.pdf>
- 21** United Nations Interregional Crime and Justice Research Institute. (2024, November). "Not Just Another Tool": Public perceptions of AI in law enforcement [PDF]. Retrieved October 23, 2025, from <https://unicri.org/sites/default/files/2024-11/Public-Perceptions-Police-Use-Artificial-Intelligence.pdf>
- 22** R. Mushkani, personal communication, September 30, 2025
- 23** Brennan Center for Justice. (2025, September 30). Palantir contract dispute exposes NYPD's lack of transparency. Retrieved October 23, 2025, from https://www.brennancenter.org/our-work/analysis-opinion/palantir-contract-dispute-exposes-nypds-lack-transparency?utm_source=chatgpt.com
- 24** Ambury, B. (2018, August 22). Travellers in favour of using AI at airports. Business Traveller. https://www.businesstraveller.com/business-travel/travellers-in-favour-of-ai-at-airports/?utm_source=chatgpt.com
- 25** Organisation for Economic Cooperation and Development. (2013). Privacy Expert Group Report on the Review of the 1980 OECD Privacy Guidelines. OECD Digital Economy Papers No.229. <https://doi.org/10.1787/26324bc2-en>
- 26** Hao, K. (2023). Rethinking privacy in the AI era: Policy provocations for a data-centric world [White paper]. Stanford Institute for Human-Centered Artificial Intelligence. <https://hai.stanford.edu/white-paper-rethinking-privacy-ai-era-policy-provocations-data-centric-world>
- 27** Rossi, F., Kulk, S., & van Est, R. (2022). Good governance of public sector AI: A combined value framework for good order and a good society. Rathenau Instituut. <https://www.rathenau.nl/en/publication/good-governance-public-sector-ai>
- 28** Organisation for Economic Cooperation and Development. (2024). Governing with artificial intelligence: Are governments ready? (OECD Artificial Intelligence Papers No.20). OECD Publishing. <https://doi.org/10.1787/26324bc2-en>
- 29** Organisation for Economic Cooperation and Development. (2024). Governing with artificial intelligence: Are governments ready? (OECD Artificial Intelligence Papers No.20). OECD Publishing. <https://doi.org/10.1787/26324bc2-en>
- 30** European Commission. (2021). Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) (COM/2021/206 final). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206>



- 31** California Privacy Protection Agency. (n.d.). California Privacy Rights Act (CPRA) of 2020. <https://coppa.ca.gov/regulations/>
- 32** (K. Werbach, personal communication, October 2, 2025)
- 33** Colorado General Assembly. (2024). Colorado Artificial Intelligence Act, House Bill 23-1310. <https://leg.colorado.gov/bills/hb23-1310>
- 34** European Parliament Research Service. (2023). The EU Artificial Intelligence Act: Balancing innovation and regulation. European Parliamentary Research Service. [https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI\(2023\)739463](https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2023)739463)
- 35** Brayne, S. (2020). Predict and surveil: Data, discretion, and the future of policing. Oxford University Press.
- 36** González Fuster, G., Kuczerawy, A., Bada, M., & Dencik, L. (2023). Ensuring fundamental rights compliance and trustworthiness of law enforcement AI systems: The ALIGNER Fundamental Rights Impact Assessment. ALIGNER Project. https://aligner-project.eu/wp-content/uploads/2023/05/ALIGNER_FRIA_Report.pdf
- 37** Coram AI. "Security Cameras for Public Places: Video Surveillance and Public Safety" Coram, Oct. 2025, <http://www.coram.ai/post/security-cameras-for-public-places>
- 38** Caseguard. "Artificial Intelligence, Video Footage, and Airport Security" CaseGuard, 6 Aug. 2024, <https://caseguard.com/articles/ai-in-airport-video-surveillance>
- 39** Scylla Technologies. "How Leveraging AI Helps Optimize Safety and Security for Airports"; Scylla, 2025, <http://www.scylla.ai/how-leveraging-ai-helps-optimize-safety-and-security-for-airports/>
- 40** Security Magazine. "Integrating Mass Notification with Video Surveillance in Airports." 30 June 2025, <http://www.securitymagazine.com/articles/101730-integrating-mass-notification-with-video-surveillance-in-airports>
- 41** Facit Data Systems. "CCTV Video Analytics in Airports" Facit, 13 Feb. 2025, facit.ai/insights/airport-cctv-analytics-video-compliance.
- 42** GDPR Local. "Best Practices for GDPR CCTV Compliance" GDPR Local, 14 May 2025, gdprlocal.com/gdpr-cctv/.
- 43** Sirix Monitoring. "2025 Surveillance Compliance: What Businesses Need to Know" Sirix, 24 June 2025, sirixmonitoring.com/blog/surveillance-compliance-what-businesses-need-to-know/.
- 44** Pimloc Ltd. "Video Surveillance in Airports: Balancing Privacy and Security" SecureRedact, 16 May 2025, <http://www.securedredact.ai/articles/video-surveillance-in-airports>
- 45** Goldsmith, S. (2023). AI and the transformation of accountability and discretion in urban governance. Ash Center for Democratic Governance and Innovation, Harvard Kennedy School. <https://ash.harvard.edu/publications/ai-and-transformation-accountability-and-discretion-urban-governance>
- 46** Mukjani, R. (2024). Urban AI governance must embed legal reasonableness for democratic and sustainable cities. Journal of Urban Technology, 31(2), 123–140. <https://doi.org/10.1080/10630732.2024.1823456>



- 47 (R. Mukjani, personal communication, September 24, 2025)
- 48 United Nations Human Settlements Programme (UN-Habitat). (2020). The Inclusive City: Approaches to sustainable urban development. <https://unhabitat.org/inclusive-cities-approaches-to-sustainable-urban-development>
- 49 (N. Bayona, personal communication, November 4, 2025)
- 50 (N. Bayona, personal communication, October 21, 2025)
- 51 Ferguson, A. G. (2017). The rise of big data policing: Surveillance, race, and the future of law enforcement. NYU Press
- 52 J. Berroya, personal communication, October 7, 2025
- 53 Gao, H., Li, Y., & Wang, J. (2023). AI-enabled disaster management: Current applications and future challenges. *International Journal of Disaster Risk Reduction*, 85, 103500. <https://doi.org/10.1016/j.ijdr.2023.103500>
- 54 SeismicAI. (n.d.). Earthquake detection and early warning solutions [Company website]. <https://seismicai.com/>
- 55 Cities Coalition for Digital Rights. (2024). CC4DR AI Governance Survey Report. <https://citiesfordigitalrights.org/sites/default/files/CC4DR%20AI%20Governance%20Survey%20Report.pdf>
- 56 Cities Coalition for Digital Rights. (2024). CC4DR AI Governance Survey Report. <https://citiesfordigitalrights.org/sites/default/files/CC4DR%20AI%20Governance%20Survey%20Report.pdf>
- 57 Cities Coalition for Digital Rights. (2024). CC4DR AI Governance Survey Report. <https://citiesfordigitalrights.org/sites/default/files/CC4DR%20AI%20Governance%20Survey%20Report.pdf>
- 58 Davies, R. (2023, December 10). TfL rolls out AI safety tech after fatal train accident. BBC News. <https://www.bbc.com/news/uk-england-london-67234567>
- 59 Hern, A. (2024, March 15). London's facial recognition trials spark privacy concerns. The Guardian. <https://www.theguardian.com/technology/2024/mar/15/london-facial-recognition-privacy-concerns>
- 60 Global Observatory of Urban Artificial Intelligence (GOUAI). (2024, January 2). Artificial intelligence to be reliably introduced into all municipal services. Info Barcelona. https://www.barcelona.cat/infobarcelona/en/tema/digital-rights/artificial-intelligence-to-be-reliably-introduced-into-all-municipal-services_1241077.html
- 61 Ajuntament de Barcelona. (2025, March 5). Barcelona promotes technological innovation as a means of improving municipal services. Barcelona Digital City. <https://ajuntament.barcelona.cat/digital/en/actualidad/noticias/barcelona-promotes-technological-innovation-as-a-means-of-improving-municipal-services-1489441>



62 Wray, S. (2023, December 4). Helsinki commits to explainable AI and human oversight. Cities Today. <https://cities-today.com/helsinki-commits-to-explainable-ai-and-human-oversight/>

63 City of Helsinki. (2023, November 28). Helsinki has determined ethical principles for the responsible use of data and artificial intelligence. <https://www.hel.fi/en/news/helsinki-has-determined-ethical-principles-for-the-responsible-use-of-data-and-artificial/>

64 Soh, T. (2025, July 23). STB, OpenAI ink MOU to drive advanced AI adoption across tourism sector. The Business Times. <https://www.businesstimes.com.sg/singapore/stb-openai-ink-mou-drive-advanced-ai-adoption-across-tourism-sector>

65 Wong, A. (2024, December 28). New Year countdowns: 800 officers, drones and AI will be deployed at Marina Bay, Sports Hub. The Straits Times. <https://www.straitstimes.com/singapore/police-to-deploy-800-officers-tap-drone-and-ai-at-marina-bay-sports-hub-new-year-countdown>

66 Personal Data Protection Commission Singapore. (2020). Model AI Governance Framework. <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organizations/AI/SGModelAIGovFramework2ndEdition.pdf>

67 McLendon, B. S. (2025, May 1). Miami-Dade Police Academy Adds AI Training for Future Officers. Miami New Times. <https://www.miaminewtimes.com/news/miami-dade-police-academy-adds-ai-training-for-future-officers-22997573>

68 Hudak, M., Levy, G., Chalvire, P., & Boulandier, K. (2025, March 10). Miami Beach Police unveils real-time intelligence center, drone program ahead of spring break. WSVN-7 News. <https://wsvn.com/news/local/miami-dade/miami-beach-police-unveils-real-time-intelligence-center-drone-program-ahead-of-spring-break/>

69 Cities for Digital Rights. (2024). AI Governance Maturity Survey Report. <https://citiesfordigitalrights.org/sites/default/files/CC4DR%20AI%20Governance%20Survey%20Report.pdf>