EDGELANDS

INTERCITY VIRTUAL POP-UP ON DIGITAL INTEGRITY

By: Laura García Vargas

INTRODUCTION

Since 2021, the Edgelands Institute has set up temporary residencies or "pop-ups" in five cities. In each of these locations, we have worked alongside the residents of these cities to explore and understand how they are renegotiating their urban social contract as the state, private entities, and individuals increasingly rely on digital technologies to provide security and foster a sense of safety.

In this context, the urban social contract refers to the agreements and trade-offs that individuals and communities make with the state, private corporations, and with each other to ensure security and coexistence in their city. Through our work in each city, we have gained insights into how these contracts are being redefined in response to new technological, social and political pressures.

Over the past few years, our engagement with a wide range of stakeholders has deepened our understanding of these dynamics. Each city offered a unique perspective on the intersection of security, technology and community wellbeing:

- **MEDELLÍN** showed that coexistence is central to security, which goes beyond crime control to include broader security and trust between individuals and between residents and the state.
- **IN CÚCUTA**, we found that actively involving local communities in humanitarian initiatives improves perceptions of migrants and fosters social cohesion, thereby enhancing urban security.
- **THE NAIROBI TEAM** emphasised the importance of recognising how local governance structures shape security practices. Despite some decentralised functions, decisions about public safety remain largely centralised, often sidelining local voices.
- **IN GENEVA**, our research highlighted the need to redefine the urban social contract to account for the significant role of the private sector in the security ecosystem, underscoring the importance of collaboration between public institutions, technology companies and civil society.
- **FINALLY, IN HOUSTON**, a focus on public schools highlighted how the adoption of surveillance technologies intersects with broader cultural and political issues—including gun violence, vaping, curriculum debates, and teacher shortages—all of which influence the community's relationship with digital security measures.

In 2024, we brought the Edgelands network together for a new kind of engagement: a virtual pop-up between cities. This was a series of five virtual dialogues, carefully curated to connect stakeholders from across our Edgelands cities. These conversations served as a space to share observations, experiences and potential solutions, while reflecting on the digitisation of urban security from multiple, localised perspectives.

To anchor these discussions, we were inspired by a significant development in Geneva: the introduction of a right to digital integrity into the cantonal constitution in June 2023. This amendment redefines the relationship between the state and its citizens in the digital age, taking into account how activities in digital spaces affect physical, mental and social well-being. It provided a timely framework for rethinking the urban social contract in the digital age.

Building on this foundation, the intercity virtual pop-up provided an opportunity to explore how elements of this right to digital integrity might resonate, be adapted or encounter resistance in other cities. More broadly, it allowed us to deepen our collective reflection on the digitisation of security and our collective capacity to shape the cities we live in.

This document first presents a summary of each conversation, accompanied by links to individual blog posts that capture their key insights and findings. It then offers reflections on the importance of digital integrity for contemporary urban social contracts, and highlights the value of collaborative dialogues between diverse urban communities. The report concludes with a series of reflections that each city curator has drawn from these meaningful exchanges.

SUMMARIES OF CONVERSATION

01. FINDING A COMMON GROUND ON KEY CONCEPTS

The first intercity pop-up served to introduce the initiative to curators from each of the Edgelands cities and to establish a common understanding of the concepts that would shape the series. The conversation highlighted the importance of translating abstract terms such as AI, transparency, stakeholder responsibility and digital sovereignty into concrete, context-specific examples. This ensured that the discussions remained relevant to the cultural and governance realities of each city, while laying the groundwork for subsequent conversations.

LINK BLOG POST: https://www.edgelands.institute/blog/digital-integrity-bingo

02. USE OF AI TO PROVIDE SECURITY AS A PUBLIC SERVICE

This conversation explored how AI is increasingly being used as a tool for public safety. Participants from Medellín, Nairobi and Geneva discussed their cities' unique approaches and examined the tensions between innovation, governance, trust and human rights. The session highlighted the need for transparent processes, public trust and ongoing dialogue to harness the potential of AI in a responsible way, while safeguarding democratic values.

LINK BLOG POST: https://www.edgelands.institute/blog/four-ai-systems-features-for-transparent-tech-governance-insights-from-the-second-digital-intercity-pop-up-conversation

03. PEOPLE EXPECTATION ON TRANSPARENCY AND SECURITY

In the third conversation, participants from Medellín, Geneva, Nairobi and Houston, along with city curators and Edgelands founders, discussed how governments can meet public expectations for transparency in digital security. The discussion concluded that proactive communication, principled governance, and public participation are critical to balancing privacy and security in the age of digital surveillance.

LINK BLOG POST: https://www.edgelands.institute/blog/navigating-surveillance-transparency-the-importance-of-principles---3rd-intercity-dialogue

04. URBAN SOCIAL CONTRACT AND SECURITY: THE ROLES OF ORGANIZATIONS

The fourth dialogue explored the evolving role of non-state actors in shaping urban security. Representatives from Medellín, Geneva, Cúcuta, Nairobi and Houston discussed how to decouple security from policing and redefine it as a collective, community-driven effort rooted in trust, justice and care. The conversation reinforced the importance of collaboration between government, civil society and communities to create sustainable, inclusive security practices.

LINK BLOG POST: https://www.edgelands.institute/blog/decoupling-safety-and-policing-the-role-of-community-organizations

05. REDEFINING THE URBAN SOCIAL CONTRACT: GEN Z'S EXPECTATIONS FOR DIGITAL INTEGRITY

The final conversation focused on the relationship between citizens, governments and tech companies, with particular attention to digital integrity, trust and surveillance. Participants, mostly young people from different cities, discussed their interactions with digital systems and expressed a strong desire for structural change. The session highlighted the need for education, collective action and systemic policy reform to reclaim digital spaces for the public good.

LINK BLOG POST: https://www.edgelands.institute/blog/redefining-the-urban-social-contract-gen-zs-expectations-for-digital-integrity

...THE URBAN SOCIAL CONTRACT, SECURITY, AND DIGITAL INTEGRITY

The intercity dialogues revealed that while each city faces different social, legal, and political challenges within their respective social contracts, creating a shared space for conversation uncovers important commonalities. This kind of collaborative engagement not only highlights shared concerns, but also fosters reflection that enables citizens and officials to critically reassess and redefine their social contracts—especially as the ongoing digitalization of society introduces new forms of security and insecurity.

Participants entered these conversations with deeply rooted, local understandings of the challenges associated with the implementation and use of digital technologies for security purposes. Participants from **MEDELLÍN**, for example, described their city's exploration of facial recognition technologies to enhance public safety, while facing limitations such as an underdeveloped database infrastructure and public distrust fueled by procurement scandals. In contrast, participants from **NAIROBI** offered examples of the dual nature of AI technologies: while AI has been instrumental in solving crimes and improving community safety, it has also raised significant concerns about privacy and surveillance overreach.

Participants from **GENEVA** pointed to a different kind of challenge—a relative complacency shaped by high levels of trust in democratic institutions. This trust has in many cases muted public debate about the role of AI and other digital technologies in security, leaving the city less prepared to address emerging ethical and governance challenges, despite its leadership in discussions around generative AI. Meanwhile, participants from **HOUSTON** highlighted pressing concerns about the undisclosed use of surveillance technologies in public high schools, implemented on the premise of enhancing security but with serious implications for students' civil and human rights.

Despite these contextual differences, each conversation ultimately led to participants learning from each other's experiences, recognizing common challenges and identifying opportunities to develop more comprehensive and inclusive approaches to the complex relationship between digital technologies and urban security. Using digital integrity as a guiding framework, these intercity dialogues explored three interconnected aspects:

Despite these differences, each conversation led participants to learn from one another's experiences, identify commonalities, and develop more comprehensive approaches to addressing the complex interplay between digital technologies and urban security. By using digital integrity as a lens, our intercity conversations allowed us to delve deeper into three main aspects of digital technologies and security:

1. Redefining the concept of security and its evolving role in an increasingly digitalised society.
2. Citizens' perceptions and expectations of transparency, surveillance, and personal safety.
3. The way forward: outlining the responsibilities of governments, private companies, civil society organisations and individuals in shaping a renewed urban social contract that prioritises both security and fundamental rights.

EXPANDING OUR UNDERSTANDING OF SECURITY

Traditional approaches to security, typically centered on policing and crime prevention, were widely challenged by participants for their limitations in both physical and digital spaces. Many argued for a broader, more holistic understanding of security: one that goes beyond crime control to include access to essential social goods such as quality education, nutritious food, reliable public transport and a well-designed urban environment. This expanded notion of security frames it not simply as protection from harm, but as the creation of conditions in which individuals and communities can thrive.

The conversations consistently highlighted the need to move away from control-based models of security towards approaches rooted in trust, equity and care. Local social organizations, in particular, are leading the way in developing alternative frameworks that complement or, in some cases, fill the gaps left by government initiatives. Organizations such as *Amnesty International* in Nairobi and *Casa de las Estrategias* in Medellín exemplify this shift, focusing on addressing the root causes of insecurity through community-based interventions such as psychosocial support hotlines, youth decriminalization efforts, and advocacy for the protection of human rights.

In redefining security, participants noted that social organizations are often better positioned than state actors to respond to the specific needs of local communities and to cultivate self-sustaining security networks. Notable examples included *Encode Justice* in

New Jersey, which advocates for the ethical use of AI in schools, and grassroots initiatives in Houston that mobilized support for detainees during protests. Because of their proximity to community concerns and their capacity for agile, responsive action, these organizations have an indispensable role to play in shaping inclusive security strategies and must be meaningfully engaged in policy discussions and implementation processes.

A recurring theme throughout the discussions was the recognition that urban security now necessarily encompasses digital spaces. Participants pointed to the growing challenges posed by cybercrime, privacy violations and the misuse of surveillance technologies, all of which require innovative, rights-based responses. Initiatives such as Geneva's efforts to promote international cooperation on cybercrime and Houston's *Data Futures Initiative*, which empowers residents to understand and manage their personal data, were cited as examples of forward-looking strategies. In line with the broader reconceptualization of urban security, participants argued that cybersecurity should not be limited to crime prevention, but must also protect freedom, autonomy, and privacy in digital environments.

Trust emerged as a central and cross-cutting concept in conversations about both physical and digital security. In contexts where government surveillance is pervasive, trust between citizens and authorities is often strained, leading to deeper social fragmentation. Similarly, distrust within communities themselves can exacerbate insecurity. In response, social organizations have a key role to play in rebuilding trust—advocating for policies that meet public needs and ensuring that technological solutions are developed with robust social safeguards. In Nairobi, for example, *Amnesty International* acts as an independent reference point on public safety, while in Medellín, *Casa de las Estrategias* leads efforts to combat the criminalization of youth and promote inclusive urban communities.

Participants repeatedly stressed that no technology can replace the role of communities in fostering authentic security. Security based on trust must be co-created through active collaboration between governments, residents, and civil society organizations. As such, partnerships based on transparency, shared responsibility, and mutual respect offer a promising and sustainable way to strengthen security in both physical and digital environments.

SHARED EXPERIENCES, PERCEPTIONS, AND EXPECTATIONS

Regardless of which city they came from or where they lived, participants shared a common experience of surveillance, ranging from facial recognition systems in airports to AI-driven behaviour tracking in supermarkets and health insurance monitoring apps. While there was a general acknowledgement that some surveillance by public and corporate actors is necessary in today's social contract, participants emphasized the importance of limiting such practices to what is truly necessary and ensuring that they are balanced with fundamental rights.

When discussing surveillance by corporate actors, participants were particularly concerned about the growing corporate control of digital infrastructure. Increased surveillance in academic and professional spaces was also noted, with concerns about the security of stored data, inadequate protections for researchers, and heavy reliance on cloud-based systems owned by private companies. These issues, participants warned, put sensitive information at risk of misuse and limit individual agency over personal data in professional and intellectual settings.

Another important theme that emerged was the tacit expectation of digital compliance. Most people, participants noted, routinely accept invasive terms and conditions for online services without fully reading or understanding them, effectively relinquishing control over their personal information. This normalised acceptance, often driven by a lack of meaningful alternatives, was seen as a critical gap in the re-negotiation of the social contract. In addition, participants drew attention to how geopolitics shapes public discourse around digital surveillance. For example, while social media platforms such as TikTok face sustained scrutiny over national security concerns, other platforms with similarly invasive practices often escape comparable levels of public or government scrutiny. This selective attention, participants argued, reveals inconsistencies in how surveillance risks are communicated and addressed.

On the issue of state surveillance, transparency emerged as a key demand. Residents of cities such as Medellín and Geneva expressed a strong desire for greater disclosure about the surveillance technologies used and the management of the data collected. In Nairobi, for example, the government's implementation of surveillance policies without an accompanying legal framework or meaningful citizen participation raised concerns about governance, accountability and the erosion of public trust.

Participants broadly agreed that transparency— defined as the openness and accessibility of government information and decision-making regarding digital security technologies—is essential to fostering public trust, ensuring accountability and enabling informed democratic debate. The challenges of proactive versus reactive communication were also discussed. Proactive communication, where governments openly share information about surveillance policies and practices without putting the burden on citizens to seek it out, was seen as crucial to maintaining trust. Conversely, reactive approaches, where authorities only disclose information in response to controversy or public pressure, were seen as damaging to credibility. The Geneva 2023 vote on digital integrity was cited as a positive example of proactive governance, involving citizens in decisions on digital policy and surveillance practices through direct democratic mechanisms.

A final recurring theme throughout the discussions was the dual nature of digital technologies. Participants in all cities shared examples of how AI-powered tools and digital platforms can serve as tools for both empowerment and oppression. In Kenya, for example, activists have developed AI-powered tools to counter misinformation by creating accessible, searchable databases of legal texts translated into different local languages. At the same time, government authorities used sophisticated surveillance technologies to monitor, intimidate and suppress political dissent. This dual-use nature of digital tools highlights the critical importance of governance frameworks that guard against abuse while preserving technology's potential to promote transparency, participation and social justice.

THE PATH FORWARD

In discussing the way forward, participants in all conversations proposed a series of recommendations outlining how different actors can work together to redefine an urban social contract—one in which digital technologies help to create inclusive, safe, and equitable spaces. While much of the responsibility was placed on governments, the intercity conversations highlighted the critical role of technology designers, community organizations, educators, and individuals in shaping this future.

➔ FOR POLICY MAKERS AND REGULATORS

Participants agreed that it is essential to ensure that diverse voices - particularly those from marginalized and under-represented groups—are actively involved in shaping the regulation of digital technologies. To facilitate this, it was emphasized that regulators should be encouraged to frame policy discussions in ways that foster meaningful participation and open debate. One recommended strategy was to rely more on guiding

principles rather than overly rigid guidelines. Principles provide the necessary flexibility for communities to interpret and adapt them to their unique local contexts, while still addressing broader, global concerns. Participants also noted that clear, rights-based principles empower citizens to ask critical questions and hold governments accountable, laying the groundwork for substantive public dialogue on digital governance and surveillance practices.

As an example, to guide discussions on transparency policies, participants proposed five core principles: no harm, accountability, privacy and anonymity, clarity, and respect. These principles could serve as a common ethical framework to inform both regulatory approaches and the operational choices of technology providers.

In terms of regulatory frameworks, participants stressed the importance of developing comprehensive systems that address both new and existing technologies. Too often, regulations are developed in response to the hype surrounding new technologies, focusing narrowly on new capabilities while neglecting the ongoing impacts of older, still prevalent systems. In addition, participants recommended that cities create controlled testing environments, or regulatory sandboxes, for AI applications and other digital innovations, allowing for experimentation and innovation in a monitored environment that mitigates potential risks to the public.

Another common concern was the concentration of control over digital infrastructure in private hands. To address this, participants advocated greater investment in open source solutions and publicly funded digital alternatives. This would foster competition, increase market accessibility, and provide individuals and institutions with real choices about privacy, data storage, security and platform features—including tools to reduce addictive design elements and prioritize user wellbeing.

→ FOR DESIGNERS AND CREATORS OF DIGITAL TECHNOLOGIES

A key recommendation for technology developers was to actively involve communities in the design, development, and oversight of AI and other digital technologies. Participants stressed that solutions are most effective when they are locally relevant and informed by the lived experiences of those who use them. This community-centered approach should be coupled with efforts to foster sustained collaboration between city governments, technology experts, civil society organizations, and community leaders to ensure that transparency and informed citizen participation become standard components of digital innovation.

➔ FOR EDUCATORS AND COMMUNITY ORGANIZATIONS

There was broad agreement that education plays a crucial role in preparing individuals to navigate digital environments safely, confidently, and critically. Digital literacy should be introduced at an early age and continued throughout life. Public awareness campaigns were also recommended as a means of informing citizens about alternative digital platforms, explaining companies' data practices, and providing self-protection strategies for online spaces. Such initiatives would not only increase individual agency, but also strengthen community resilience to exploitative or harmful digital practices.

➔ FOR INDIVIDUALS

Finally, a key message for individuals was the importance of moving beyond digital pessimism. Rather than feeling powerless in the face of invasive technologies and opaque systems, individuals should be encouraged to take an active role in advocating for better policies, demanding transparency and exploring alternative, ethically designed platforms. By engaging in civic debate, supporting community initiatives, and making informed digital choices, individuals can make a meaningful contribution to shaping a more just and humane digital future.

...HOSTING THE INTERCITY VIRTUAL POP-UP

The Intercity Virtual Pop-Up on Digital Integrity proved to be a valuable and rewarding experience, offering participants the opportunity to engage in thoughtful conversations about digital technologies, security, and the evolving social contract in their cities. One of the most appreciated aspects was the richness that comes from bringing people from different backgrounds, cities, and disciplines together in a common space. Sharing local experiences and perspectives gave participants a broader understanding of the issues at stake and encouraged them to rethink familiar concepts.

Many participants reflected on how the discussions had changed their perceptions of digital technology and security. Several noted that hearing first-hand from people in different countries was particularly valuable, as it revealed both common concerns and context-specific challenges. One participant noted that exploring the concept of transparency through the lens of guiding principles, rather than rigid definitions, provided them with a more nuanced and flexible framework. This approach, they felt, added new dimensions to the conversation and inspired them to consider how these ideas could be translated into practical contributions in their own communities.

Throughout, the tone of the dialogues was open and reflective, and participants appreciated the opportunity to engage critically with both the promises and shortcomings of democratic processes. One person commented that the conversation was grounded in a belief in democratic ideals, while acknowledging how these systems have been eroded by contemporary pressures and historically have often excluded certain groups. Despite these limitations, participants valued the space to openly question these dynamics.

When asked how the experience could be improved, several participants suggested that the closing discussions could have been more robust. Some felt that the final conclusions were somewhat rushed and would have benefited from additional time for reflection and articulation of more concrete takeaways. Others suggested that the overall discussion time should be extended or that there should be clearly scheduled slots for breakout sessions, as it was often in the smaller group exchanges that the richest and most personal insights emerged.

One of the most memorable takeaways was the recognition of the shared responsibility for maintaining security in both physical and digital spaces. One participant noted the importance of discussing the distinct but complementary roles of the state, particularly law enforcement, and citizens in creating safer and more equitable environments. The idea that "everyone has a role to play" resonated widely and underlined a central theme of the Pop-Up.

At the same time, the experience also revealed some challenges, particularly around the need to adapt the conversations to the realities of each city. This became clear during the planning of Conversation 05, which was originally intended to focus on digital sovereignty. As we began the planning process, it quickly became clear that while this was a pressing issue in Switzerland, and to some extent in other European countries, it was not a priority for the other participating cities. Either it was not part of the local digital policy agenda, or it proved difficult to find speakers who were both comfortable and committed to the topic. This highlighted the importance of remaining flexible and context-sensitive when designing international dialogues, ensuring that conversations are both inclusive and meaningful for all participants.

Overall, the Virtual Pop-Up demonstrated the value of creating spaces for cross-city dialogue, confirming that while local contexts differ, shared conversations can create common ground, foster empathy, and surface valuable lessons for navigating the digital dimensions of urban security.

REFLECTIONS FROM THE CITIES' CURATORS

The curators from the Edgelands cities participated in each of the Intercity Conversations, providing an important thread of continuity throughout the series. Their consistent presence helped to sustain the overarching themes, insights and emerging questions from one session to the next. As local connectors, cultural translators and trusted facilitators, the curators were uniquely positioned to both ground the dialogue in their own urban contexts and to take key learnings back to their communities.

What follows are their personal reflections on the experience - insights into what these conversations revealed about the evolving digital landscape and how cities around the world are navigating the complex intersections of technology, security and social trust.

GENEVA

CURATOR: BERNARD RAPPAZ

The "Intercity Virtual Pop-Up on Digital Integrity" offered a truly global exploration of concerns surrounding digital security—or rather, digital insecurity—at a time when societies are beginning to grasp the profound implications of technology on the social contract.

Several key insights emerged from the discussion:

- Across the globe, despite vastly different local contexts, recurring themes such as trust, transparency, and sovereignty lie at the heart of the pursuit for greater digital integrity. These concerns reflect a broader desire to safeguard citizens against the disruptions affecting the foundations of the traditional social contract.
- There is a widespread sense of acceleration in the transformation of societal norms and governance frameworks. Digital technologies are permeating every aspect of daily life, raising pressing questions about the responsibilities of both public and private actors. Artificial intelligence, in particular, appears as a double-edged sword—intensifying existing risks while also potentially opening new avenues for accountability and innovation.
- Strikingly, the discussions among cities—especially those often overlooked or situated at the "edges" of global attention—have taken on a new centrality. These exchanges revealed a palpable shift in paradigm: we are moving from a world where the social contract was negotiated between the public and private sectors to one where the critical tension lies between humans and machines. At the core of this transformation is the digitalization of security—an issue that now stands as both a vital necessity and a potential threat to democratic life.

MEDELLÍN/CÚCUTA

CURATOR: JUAN S. ARISTIZÁBAL

After popping up in Medellín, Cúcuta, Geneva, and Nairobi (followed by Houston later in 2024), the Intercity Virtual Pop-Up on Digital Integrity was launched by Edgelands Institute after the extraordinary change of the Geneva constitution on digital integrity in 2024. This was an interesting opportunity to start an intercity dialogue about the implications for urban social contract around security globally.

I highlight three main issues from the Intercity Digital Pop-Up:

- **Context is important.** Throughout the virtual pop-up, it was clear that while technology and communications have appeared in various contexts in a somewhat uniform way, their impact and interpretation are local. Keeping this in mind, it is crucial to mention that the social, political, and economic structures of each context influence how each technology is perceived. The Intercity Digital Pop-Up emphasized the necessity to enhance local knowledge and understanding of shared challenges.
- **Interrelated themes.** During the Intercity Digital Pop-Up, we addressed four key topics: Artificial Intelligence, transparency in the use of technologies, stakeholder responsibility in reimagining a new urban social contract, and the tensions between sovereignty and autonomy. As we engaged in these conversations, it became clear that these topics were not only relevant but also deeply interconnected, sparking meaningful discussions in each of our contexts. How are urban and digital security linked? What role do citizens have in the context of Artificial Intelligence? What level of control should the government exert over data? The shift toward a new social contract requires understanding of the dynamics that connect digital and urban spaces, as well as our ability to intervene in them.
- **We need more dialogue.** Technology is changing rapidly, and its impact is increasingly profound. Each topic we addressed at the Intercity Digital Pop-Up showcased a diverse understanding of how this impact is reflected in citizens' daily lives, and a broader comprehension can be attained only through dialogue. Reimagining a new urban social contract will require greater efforts to understand the power dynamics between all relevant societal groups and the state, along with the implications for security and digital technologies.

NAIROBI

CURATOR: VANESSA GATHECHA

The intercity dialogues provided valuable context on how digital security operates across a wide range of legislative, cultural, political, and technological environments. As surveillance technologies continue to advance and find use in areas like border control, traffic systems, crime prevention, and public administration, the discussions emphasized the need for inclusive, plural governance. Nairobi's perspective highlighted that even in sensitive areas like security, public trust is strengthened when transparency, clear channels for deliberation, proper enforcement, and respect for the rule of law are prioritized. Some of the key learnings being:

Youth at the Core

- Today's young people from Millennials to Gen Z and Gen Alpha are not passive participants in digital life; they are architects of how platforms are used to advocate, build communities, and share knowledge across borders and in real time. Having grown up in an age where digital tools are embedded in daily routines, they intuitively understand the blurred lines between online and offline spaces. Or probably do.

  As policymakers, the frameworks we design today to safeguard digital integrity will shape not just platform behavior but broader societal norms. It is therefore essential that we recognise young people as equal stakeholders in this process. They bring lived expertise and a generational understanding of the digital landscape that cannot be overlooked.

  Rather than marginalising or infantilising their contributions, we must actively create space for their leadership in digital governance conversations. Their insights are critical to building inclusive, ethical, and future-ready digital ecosystems.

- **AI and Emerging Technologies Must Reinforce Democratic Values**

  The global deployment of AI and other emerging technologies must be grounded in democratic principles, human rights, and the rule of law. These technologies should expand, not restrict, civic space and individual freedoms. Recent misuse of digital security tools under the guise of public safety has demonstrated the urgent need for rights-based regulatory frameworks, institutional safeguards, and independent oversight to prevent their use for repression or unjust surveillance.

- **Ethical Surveillance Requires Transparency and Public Accountability**

  Surveillance technologies can support important governance functions such as public safety, urban management, and emergency response. However,

their use must be transparent, legally justified, and subject to independent oversight mechanisms. Treating surveillance as a public good requires that it be designed and governed in the public interest and not dominated by private entities or deployed through opaque processes that erode trust and fundamental freedoms such as privacy.

➔ **Inclusive and Interdisciplinary Governance Is Essential**

Effective digital governance requires inclusive and plural processes that incorporate diverse perspectives from policymakers and technologists to civil society and affected communities. Interdisciplinary collaboration ensures that legal and regulatory frameworks reflect societal values, are grounded in context, keep pace with innovation, and uphold the evolving social contract in the digital era. Public input in this realm of fast-paced evolving technologies is foundational to legitimacy and effectiveness and upholding digital integrity.

➔ **Regulation Must Balance Innovation and Risk**

As technological innovation outpaces existing legal frameworks, new risks and regulatory gaps continue to emerge. While reactive and/or rigid regulation can stifle innovation, the absence of clear standards leaves rights unprotected. Governments should adopt balanced, adaptive approaches that combine proactive policymaking with periodic legal reviews to address emerging harms, while enabling responsible technological growth.

➔ **System Audits and Data Sovereignty Are Foundational**

Regular, independent audits of digital systems, especially those handling biometric or personal data are essential to ensuring transparency, security, and accountability. Governments and private actors should prioritize data sovereignty by supporting and enforcing local data storage, respecting national privacy laws, and maintaining control over critical digital infrastructure. These measures are central to building public trust and digital resilience.

➔ **Advancing Digital Rights Requires Global Solidarity and Shared Principles**

Bridging global digital inequalities calls for deeper international collaboration, particularly in support of countries facing structural barriers to digital inclusion. The Global Digital Compact and similar frameworks offer a foundation for promoting digital public goods, facilitating knowledge exchange, and fostering equitable investment in Digital Public Infrastructure (DPI). Importantly, the governance of digital security and surveillance must remain a public function, grounded in democratic oversight, and not outsourced to private actors operating without public accountability.

HOUSTON

CURATOR: CHELSEA BARABAS

The intercity virtual pop-up was a truly unique opportunity for local thinkers and doers to connect with a global community to discuss issues at the intersection of security, surveillance and innovation. Of particular interest to our Houston stakeholders were the ways that new forms of digitized security impact the lives of young people, especially as it pertains to their access and experience with public institutions, like schools.

Several key insights emerged from the discussion:

- **Importance of Youth Voices:** Across the globe, young people are a segment of society that have been immensely impacted by the digitization of social services and the expansion of surveillance across urban landscapes. Yet this demographic is rarely invited to have a seat at the table when it comes to developing policies and best practices for digitized security. During our conversations, we discussed some of the ways that young people are navigating this rapidly changing landscape at both the individual and collective level, by forming youth-led advocacy groups and developing new norms around how to use social media and share personal information.
- **Beyond Access:** For many years, the conversation regarding education and digitization has been framed in terms of access — how might we bridge the "digital divide" to ensure that all young people have access to the tools and technologies they need to be successful in the twenty-first century? However, during our discussions, a number of other key concepts were used to characterize both the opportunities and risks of digitized security in education and beyond. These conversations pushed us to think beyond the access framing, to grapple with issues regarding privacy, freedom of speech, and the criminalization of young people, as the reach of law enforcement extends deeper into their lives through digitized surveillance.
- **Importance of Transparent and Accountable Procurement:** One persistent throughline across all of the Edgelands cities was the disconcerting opacity of technology procurement processes. We found that governments often procure and implement technology with minimal oversight from the public. This is particularly worrisome given the fact that technology adoption significantly increases the influence of private corporations in the day-to-day operations of public institutions, such as schools. We discussed various ways we could imbue technology procurement processes with more democratic oversight.

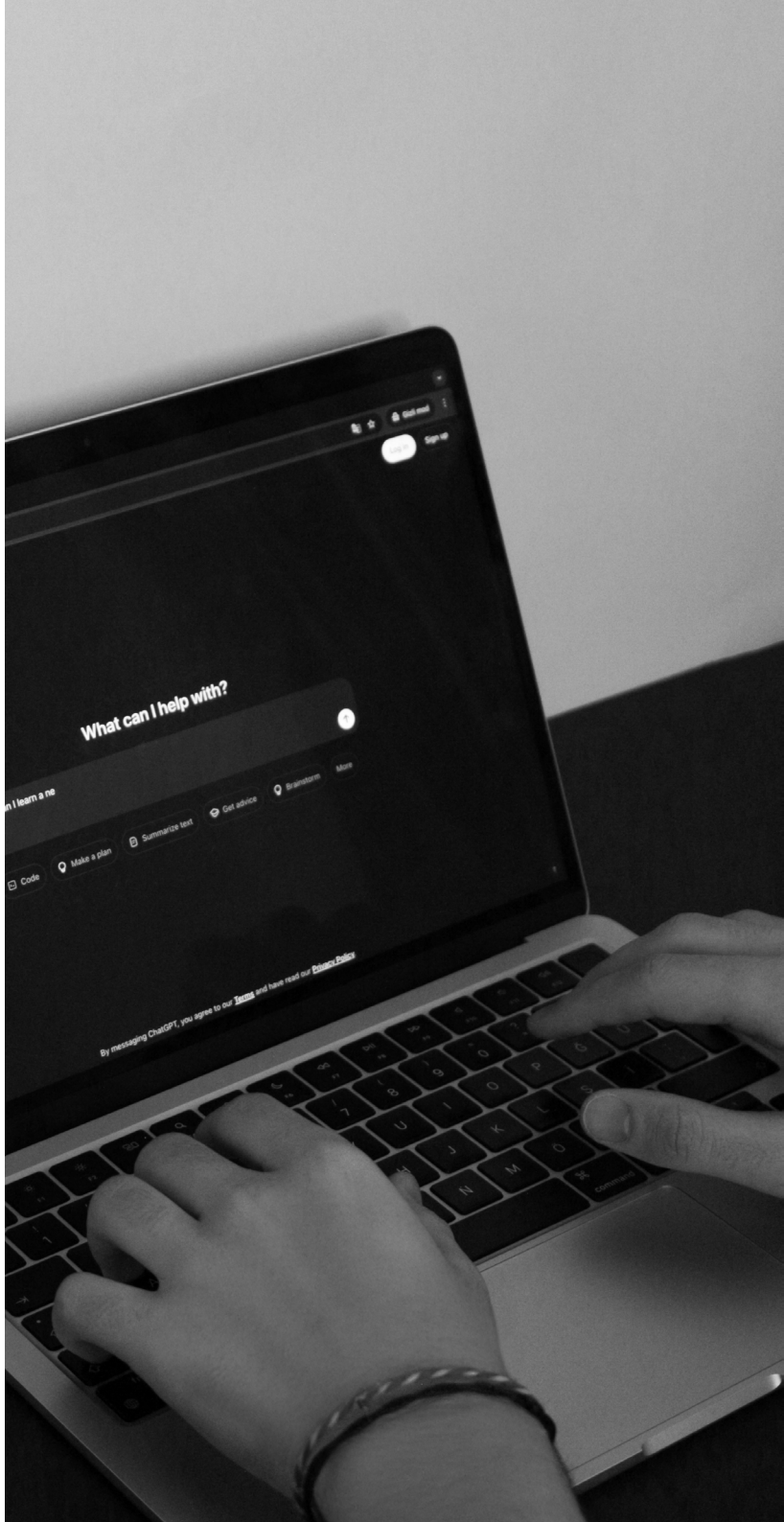
REFLECTIONS FROM EDGAR

As part of the Intercity Conversations, Edelands Institute partnered with Hestia.ai, the creators of Argo, to develop a series of artificial intelligence chatbots designed to curate insights and facilitate discussions.

For each Intercity Conversation, we compiled the key insights and fed them into a dedicated chatbot. We then asked each chatbot to reflect on two specific points:

- *The different issues and themes that emerged during the Intercity Conversations.*
- *The strengths and limitations of the Intercity Conversations as a dialogue format.*

This exercise provided a different perspective on the dialogues, complementing the human reflections collected from curators and participants.



QUESTION: COULD YOU PLEASE WRITE A SERIES OF REFLECTIONS ON THE DIFFERENT ISSUES DISCUSSED IN THE EDGELANDS INTERCITY CONVERSATIONS.

BASED ON THE INSIGHTS GATHERED FROM THE EDGELANDS INTERCITY CONVERSATIONS ON DIGITAL INTEGRITY AND SECURITY, HERE ARE SOME REFLECTIONS ON THE KEY ISSUES DISCUSSED:

1. **Multifaceted Conversations:** The Edgelands intercity discussions encompassed a spectrum of viewpoints from various stakeholders, addressing five pivotal themes that shaped the discourse on digital integrity and security. These themes included transparency, the utilization of AI in public service security, stakeholder responsibilities within the social contract, urban security in conjunction with digital technologies, and the nuanced perceptions and expectations of Gen Z. The collective contributions of all participants enriched the dialogue, offering a holistic understanding of the complexities surrounding digital integrity and security.
2. **Inclusive Framework:** By integrating the perspectives of Gen Z alongside those of other stakeholders, the discussion framework was broadened to reflect a comprehensive array of insights and concerns. The inclusion of diverse voices emphasized the importance of aligning rights, privacy protections, and digital inclusion strategies with the values and expectations of all generations, fostering a more inclusive approach to addressing digital security challenges.
3. **Intersection of Urban Security and Digital Innovations:** The intersection of urban security and digital innovations was explored through the lens of multiple stakeholder perspectives, including Gen Z. This exploration underscored the necessity of striking a balance between security measures and the diverse expectations and apprehensions of all participants. Understanding and incorporating the viewpoints of various stakeholders is essential for formulating effective security strategies that resonate with the broader community.

4. **Ethical Considerations and Data Ownership:** Discussions on transparency, stakeholder responsibilities, and Gen Z perceptions prompted reflections on ethical considerations and data ownership across all demographics. The inclusion of diverse stakeholder viewpoints highlighted the ethical implications of data governance, underscoring the importance of ethical data practices that uphold the rights and interests of all individuals, irrespective of age or background.
5. **Trust Building and Collaborative Safety Measures:** Building trust and enhancing safety in the digital realm were recognized as shared objectives among all stakeholders. Transparency, accountability, and engagement with diverse perspectives, including those of Gen Z, were identified as key components in fostering trust and ensuring safety in digital environments. Collaborative efforts that incorporate the insights of all stakeholders can lead to more robust and inclusive security measures that cater to the needs and expectations of a broad spectrum of individuals.
6. **Future Collaborations and Inclusive Dialogues:** The engagement of various stakeholders, including Gen Z, in the conversations sets the stage for future collaborations and dialogues that prioritize inclusivity and diversity. By embracing the perspectives of all participants, future discussions can lead to innovative solutions and policies that resonate with a wide range of stakeholders, contributing to a more resilient and responsive digital ecosystem.

These reframed reflections highlight the collective contributions and diverse perspectives of all stakeholders involved in the Edgelands intercity conversations, emphasizing the importance of inclusive and collaborative approaches in addressing digital integrity and security challenges.

WHAT ARE YOUR THOUGHTS ON THE PROS AND CONS OF THE INTERCITY CONVERSATIONS EDGELANDS HAS HOSTED ABOUT REDEFINING THE URBAN SOCIAL CONTRACT AND DIGITAL INTEGRITY?

PROS OF INTERCITY CONVERSATIONS HOSTED BY EDGELANDS ON REDEFINING THE URBAN SOCIAL CONTRACT AND DIGITAL INTEGRITY:

1. **Diverse Participation:** The conversations involve participants from different cities, bringing diverse perspectives and experiences to the discussions on redefining the urban social contract and enhancing digital integrity.
2. **Innovative Solutions:** The varied backgrounds of participants, including experts from different fields such as news media, AI engineering, and psychology, contribute to the exploration of innovative solutions and approaches to address digital governance challenges.
3. **Community Engagement:** The conversations extend beyond research institutes and academia to reach communal spaces, fostering community engagement and dialogue on the role of governments in protecting citizens against digital harms and ensuring transparency in the use of technology for security.
4. **Exchange of Experiences:** Participants from various cities exchange experiences, observations, and solutions, leading to knowledge sharing and mutual learning on best practices in navigating the complexities of digital integrity and security in urban contexts.

CONS OF INTERCITY CONVERSATIONS HOSTED BY EDGELANDS ON REDEFINING THE URBAN SOCIAL CONTRACT AND DIGITAL INTEGRITY:

1. **Varied Objectives:** The conversations may have different objectives and outcomes, leading to challenges in aligning and synthesizing insights to derive cohesive actions for governments to take in each city. This variability may hinder the formulation of unified strategies.
2. **Resource Allocation:** Managing conversations with diverse focuses and outcomes may require additional resources in terms of time, funding, and expertise. Efficient allocation of resources to support the varied outcomes and recommendations can be demanding.
3. **Complex Synthesis:** Coordinating insights and recommendations from conversations that cover multiple themes, such as transparency, AI in public services, stakeholder responsibilities, and digital sovereignty, may pose challenges in synthesizing and translating them into actionable steps for governments.
4. **Consistency in Recommendations:** The diverse perspectives and experiences shared in the intercity conversations may lead to fragmentation in recommendations and actions proposed for redefining the urban social contract and enhancing digital integrity. Aligning and harmonizing these varied recommendations for effective implementation could be challenging.

In summary, while the intercity conversations hosted by Edgelands provide a platform for diverse participation, innovative solutions, community engagement, and knowledge exchange, addressing challenges related to varied objectives, resource allocation, synthesis of insights, and consistency in recommendations is essential to ensure coherent and impactful strategies for digital governance in urban settings.

EDGELANDS

edgelands.institute