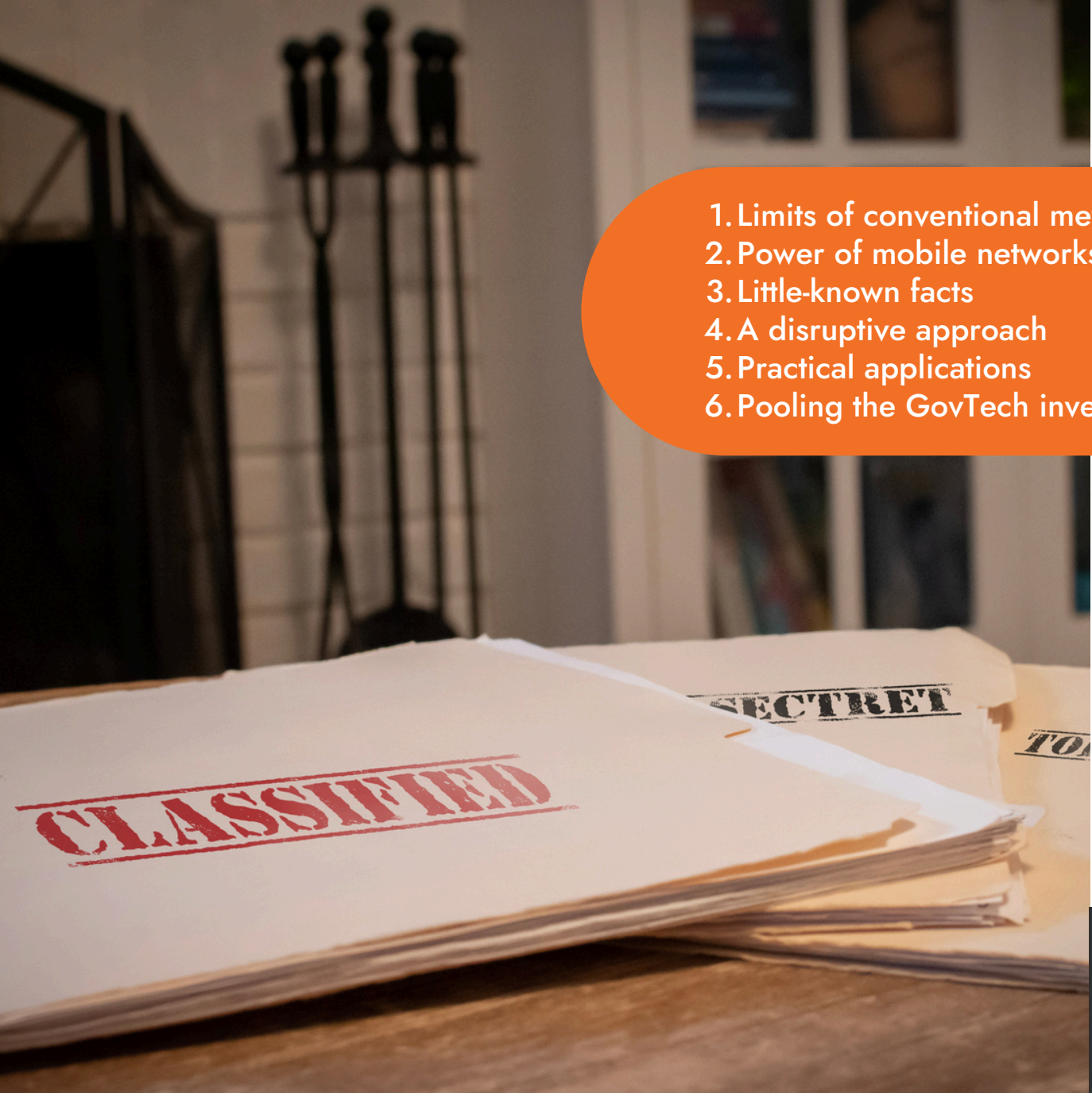


Whitepaper

GovTech: Network Intelligence for Homeland Security

- 
1. Limits of conventional methods
 2. Power of mobile networks
 3. Little-known facts
 4. A disruptive approach
 5. Practical applications
 6. Pooling the GovTech investment

Homeland security: behind the scenes



Security agencies around the world are increasingly facing a range of complex challenges: escalation of geopolitical threats, widespread cyberattacks, more and more sophisticated criminal methods with the growing use of encrypted communication apps.

“ In 2023 alone, there were 162,000 conflict-related deaths, the second highest toll recorded in the past 30 years. ”

Institute for Economics & Peace

This context highlights the need for advanced solutions to counter evolving threats. Governments are under pressure to enable proportionate investigation techniques to safeguard national security, while still respecting citizens' fundamental rights. While some nations have opted for extensive surveillance measures that often infringe on privacy, others seek more balanced approaches that prioritize legal frameworks and individual freedoms. This dichotomy highlights the ongoing debate on how best to protect citizens while respecting their rights.

1) TRADITIONAL METHODS REACH THEIR LIMITS



ID	Input	Side	AUL	AJP	RMS	Name	% Voice	% Digits	% Guard	% Info
11132149-47	E1	San Francisco	-8.237072	95.891807	-8.422083	38.188702	65.531704	0	0	2.400317
11132149-48	E1	San Francisco	-8.249787	95.920951	-8.421213	38.174495	45.51225	0	0	2.878676
11132149-49	W5	San Francisco	-8.237072	95.891807	-8.422083	38.188702	65.531704	0	0	2.400317
11132149-50	E1	San Francisco	-8.249787	95.920951	-8.421213	38.174495	45.51225	0	0	2.878676
11132149-51	W5	San Francisco	-8.249787	95.920951	-8.421213	38.174495	45.51225	0	0	2.878676
11132149-52	E1	San Francisco	-8.237072	95.891807	-8.422083	38.188702	65.531704	0	0	2.400317
11132149-53	W5	San Francisco	-8.237072	95.891807	-8.422083	38.188702	65.531704	0	0	2.400317
11132149-54	E1	San Francisco	-8.249787	95.920951	-8.421213	38.174495	45.51225	0	0	2.878676
11132149-55	W5	San Francisco	-8.249787	95.920951	-8.421213	38.174495	45.51225	0	0	2.878676
11132149-56	E1	San Francisco	-8.237072	95.891807	-8.422083	38.188702	65.531704	0	0	2.400317
11132149-57	W5	San Francisco	-8.237072	95.891807	-8.422083	38.188702	65.531704	0	0	2.400317
11132149-58	E1	San Francisco	-8.249787	95.920951	-8.421213	38.174495	45.51225	0	0	2.878676
11132149-59	W5	San Francisco	-8.249787	95.920951	-8.421213	38.174495	45.51225	0	0	2.878676
11132149-60	E1	San Francisco	-8.237072	95.891807	-8.422083	38.188702	65.531704	0	0	2.400317
11132149-61	W5	San Francisco	-8.237072	95.891807	-8.422083	38.188702	65.531704	0	0	2.400317
11132149-62	E1	San Francisco	-8.249787	95.920951	-8.421213	38.174495	45.51225	0	0	2.878676
11132149-63	W5	San Francisco	-8.249787	95.920951	-8.421213	38.174495	45.51225	0	0	2.878676
11132149-64	E1	San Francisco	-8.237072	95.891807	-8.422083	38.188702	65.531704	0	0	2.400317
11132149-65	W5	San Francisco	-8.237072	95.891807	-8.422083	38.188702	65.531704	0	0	2.400317
11132149-66	E1	San Francisco	-8.249787	95.920951	-8.421213	38.174495	45.51225	0	0	2.878676
11132149-67	W5	San Francisco	-8.249787	95.920951	-8.421213	38.174495	45.51225	0	0	2.878676
11132149-68	E1	San Francisco	-8.237072	95.891807	-8.422083	38.188702	65.531704	0	0	2.400317
11132149-69	W5	San Francisco	-8.237072	95.891807	-8.422083	38.188702	65.531704	0	0	2.400317
11132149-70	E1	San Francisco	-8.249787	95.920951	-8.421213	38.174495	45.51225	0	0	2.878676
11132149-71	W5	San Francisco	-8.249787	95.920951	-8.421213	38.174495	45.51225	0	0	2.878676
11132149-72	E1	San Francisco	-8.237072	95.891807	-8.422083	38.188702	65.531704	0	0	2.400317
11132149-73	W5	San Francisco	-8.237072	95.891807	-8.422083	38.188702	65.531704	0	0	2.400317
11132149-74	E1	San Francisco	-8.249787	95.920951	-8.421213	38.174495	45.51225	0	0	2.878676
11132149-75	W5	San Francisco	-8.249787	95.920951	-8.421213	38.174495	45.51225	0	0	2.878676
11132149-76	E1	San Francisco	-8.237072	95.891807	-8.422083	38.188702	65.531704	0	0	2.400317
11132149-77	W5	San Francisco	-8.237072	95.891807	-8.422083	38.188702	65.531704	0	0	2.400317
11132149-78	E1	San Francisco	-8.249787	95.920951	-8.421213	38.174495	45.51225	0	0	2.878676
11132149-79	W5	San Francisco	-8.249787	95.920951	-8.421213	38.174495	45.51225	0	0	2.878676
11132149-80	E1	San Francisco	-8.237072	95.891807	-8.422083	38.188702	65.531704	0	0	2.400317
11132149-81	W5	San Francisco	-8.237072	95.891807	-8.422083	38.188702	65.531704	0	0	2.400317
11132149-82	E1	San Francisco	-8.249787	95.920951	-8.421213	38.174495	45.51225	0	0	2.878676
11132149-83	W5	San Francisco	-8.249787	95.920951	-8.421213	38.174495	45.51225	0	0	2.878676
11132149-84	E1	San Francisco	-8.237072	95.891807	-8.422083	38.188702	65.531704	0	0	2.400317
11132149-85	W5	San Francisco	-8.237072	95.891807	-8.422083	38.188702	65.531704	0	0	2.400317
11132149-86	E1	San Francisco	-8.249787	95.920951	-8.421213	38.174495	45.51225	0	0	2.878676
11132149-87	W5	San Francisco	-8.249787	95.920951	-8.421213	38.174495	45.51225	0	0	2.878676
11132149-88	E1	San Francisco	-8.237072	95.891807	-8.422083	38.188702	65.531704	0	0	2.400317
11132149-89	W5	San Francisco	-8.237072	95.891807	-8.422083	38.188702	65.531704	0	0	2.400317
11132149-90	E1	San Francisco	-8.249787	95.920951	-8.421213	38.174495	45.51225	0	0	2.878676
11132149-91	W5	San Francisco	-8.249787	95.920951	-8.421213	38.174495	45.51225	0	0	2.878676
11132149-92	E1	San Francisco	-8.237072	95.891807	-8.422083	38.188702	65.531704	0	0	2.400317
11132149-93	W5	San Francisco	-8.237072	95.891807	-8.422083	38.188702	65.531704	0	0	2.400317
11132149-94	E1	San Francisco	-8.249787	95.920951	-8.421213	38.174495	45.51225	0	0	2.878676
11132149-95	W5	San Francisco	-8.249787	95.920951	-8.421213	38.174495	45.51225	0	0	2.878676
11132149-96	E1	San Francisco	-8.237072	95.891807	-8.422083	38.188702	65.531704	0	0	2.400317
11132149-97	W5	San Francisco	-8.237072	95.891807	-8.422083	38.188702	65.531704	0	0	2.400317
11132149-98	E1	San Francisco	-8.249787	95.920951	-8.421213	38.174495	45.51225	0	0	2.878676
11132149-99	W5	San Francisco	-8.249787	95.920951	-8.421213	38.174495	45.51225	0	0	2.878676



Traditional investigative methods to acquire targets' location or analyze criminal network activities are resource-intensive and bound by strict regulations:



- IMSI catchers have faced growing limitations in 5G environments.
- Call interception and wiretapping, while effective in some contexts, require significant resources and may not always deliver timely or actionable results.
- Call Data Records (CDRs), long been used by law enforcement agencies to access the location logs of mobile phones at specific times within defined areas, provide valuable insights but:
 - Location data is imprecise, with a margin of error in hundreds of meters
 - Limited data points per SIM card (only a few/day) restrict investigative depth
 - Criminals increasingly using encrypted messaging apps, reducing CDR utility
- Tower dumps offer only broad insights into call activity and require significant time to cross-check manually.

In addition, communications are increasingly encrypted, further reducing the utility of these traditional techniques. The need for more effective and efficient security solutions has never been greater, as evidenced by the increased global investment in AI-driven policing solutions, with budgets rising by an average of 28.4% annually in Europe.



The Europe AI for public security and safety market is expected to grow from US\$ 3,345.28 million in 2023 to US\$ 19,231.52 million by 2030. It is estimated to grow at a CAGR of 28.4% from 2023 to 2030.

Business Market Insights

2) MOBILE NETWORKS HAVE ENORMOUS POTENTIAL

In 2024, there will be an estimated 8.65 billion mobile connections worldwide, with smartphones accounting for 82% of all mobile devices. This means there is now more than one mobile device for every person on Earth. The scale and reach of mobile networks make them an invaluable resource for governments seeking to enhance national security.

The global connectedness enabled by ICTs has made the world more interconnected. While this has brought numerous benefits, it has also connected criminal networks, enabling coordinated activities across borders. WhatsApp, the most popular mobile messaging app, boasts 2.96 billion unique users across 180 countries.

“

In 2024, WhatsApp has surpassed 2.96 billion unique users in 180 countries, making it the most popular mobile messenger app

Statista

”



This highlights the importance of understanding mobile network behavior as a means of tracking and responding to emerging threats.

3) LITTLE-KNOWN FACTS ABOUT MOBILE NETWORKS

Mobile Network Operators (MNOs) continuously measure signal strength between base stations and handsets. This is crucial for performing basic operations of the mobile network, such as handovers, to optimize user experience. These measurements, stored in RAN logs, are essential for managing infrastructure and provide critical intelligence for network operations.

Mobile phones are constantly communicating with the network, transmitting vast amounts of signal measurements and location data.

While many security agencies analyze these logs to track the movements of individuals at a given time, the insights are often limited due to a technical challenge: the high level of processing performance required to process and analyze these logs.

In contrast, back in 2013, Intersec developed an original approach, extracting just the necessary information from the RAN through a centralized platform, in its original format. When no signaling is available for some lapse of time, a mechanism called orchestration actively triggers an updated position from the network. Such information is mixed with all networks available (including Wi-Fi) to limit the number of blind spots for any individual device.

Performance depends on the network topology but recently observed results show it can reach down to 5 meters accuracy in urban areas in near real-time, bringing along with all metadata insights that can be leveraged to enhance national security efforts.



- Each mobile device generates thousands of data points per day, providing an accurate picture of an individual's location and behavior. This comprehensive information can be used to build detailed profiles, identify patterns, and uncover hidden connections among suspects.
- AI algorithms can combine unique identifiers with real-time location information to create detailed profiles of individuals' movements and activities.
- Data from mobile networks, including that of foreign nationals, can be stored for periods ranging from six months to five years.

4) A DISRUPTIVE, ETHICAL & COMPLIANT APPROACH

As described above, in-depth metadata analysis represents a groundbreaking approach to national security. Since it utilizes anonymized data, it is less intrusive than content interception and falls within a more flexible legal framework:

- It is a more lightweight approach as it allows for large-scale digital surveillance, applying the principle of proportionality and ensuring minimal intrusion while maximizing operational benefits.
- Unlike traditional methods, which focus on the content of communications, metadata analysis studies the attributes of communication, such as who is communicating, when, where, and how.



“Metadata covers all technical data relating to communications, with the notable exception of data relating to the content of exchanges: it does not reveal the text of messages (e-mails, SMS messages, etc.) sent or received, nor the nature of remarks made during telephone conversations. With a wide range of uses for investigators (identifying the protagonists of a crime; uncovering hidden lines; identifying people present at the scene of a crime, etc.).

Network data is now a key piece of evidence, both as a starting point for investigations and as a requirement of prosecutors to ensure the credibility of the prosecution.”

2023 report from French Senate

By processing large volumes of metadata quickly, security agencies can identify potential threats and focus their efforts more effectively. This approach strikes a balance between operational effectiveness and the protection of individual liberties.

5) GAINING INSIGHTS THROUGH THE AI LENS

The Intersec approach to mobile network intelligence leverages the power of network metadata in combination with artificial intelligence (AI) to generate insights that would otherwise be difficult to uncover.

With metadata analysis, security agencies can instantly identify members of criminal groups, even if they have not made calls in specific areas or if they communicate through WhatsApp, Signal, Telegram...

AI-powered network metadata intelligence can reveal a target's patterns of life, providing insight into where they live, work, and spend most of their time. It can also help identify connections with other individuals, detect potential threats in real time, and monitor borders for unusual activity, such as the movement of foreign SIM cards. Moreover, encrypted communications are not an obstacle to this approach.

As Rémi Récio, General Delegate of CNCIS, explains:

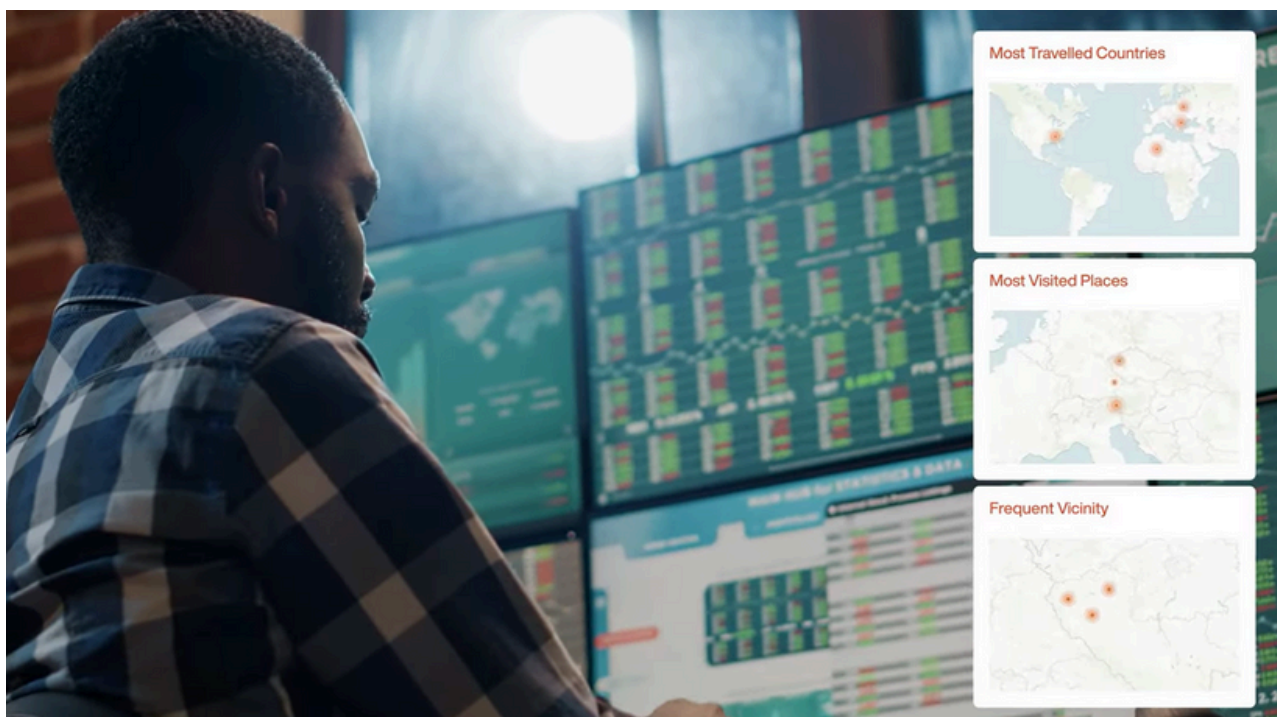
“Terrorists aren't going to openly discuss planting a bomb in a conversation. However, reconstructing networks through technical data is far more operationally useful than what people actually say.”

Slate article: “On m'écoute ou on me fadette?”



Some practical applications:

- **Missing Persons:** Metadata can provide crucial information about the last known location of missing individuals, even if their phones are switched off. The system can identify devices with similar trajectories and monitor live movements.
- **Crime Investigations:** Metadata can help identify individuals with suspicious communication patterns, reveal hidden connections, and even access suspects' locations retrospectively.
- **Strategic Site Surveillance:** Mobile network intelligence can be used to monitor sensitive sites, detect abnormal gatherings or movements, and monitor individuals from watchlists.
- **Counterterrorism:** By analyzing network activity and mobility patterns, security agencies can identify potential terrorist cells and trigger alerts when suspects enter crowded or high-risk areas, such as airports or embassies.
- **Border Control:** Monitoring SIM card activity from specific nationalities in border areas or detecting devices handed to refugees can enhance border security efforts.
- **Financial Investigations:** Metadata can also help identify suspicious financial transactions, aiding in the detection of fraud or money laundering schemes.



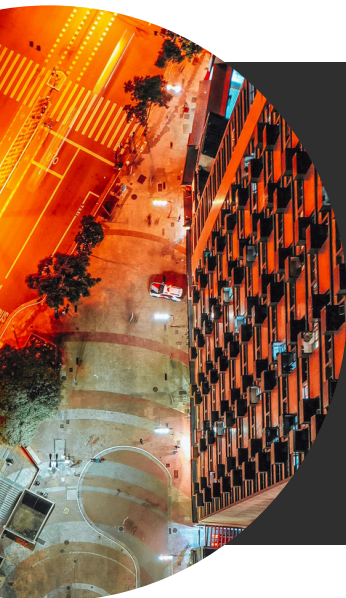
6) POOLING GOVTECH INVESTMENT

Governments are large entities that allocate significant resources to technology each year. However, they are increasingly focused on minimizing wasteful spending.

Mobile Network Metadata Analysis:

- **Can be deployed quickly and seamlessly:**
 - Utilizing mobile network metadata allows organizations to benefit from an existing sensor network, unlike solutions that require the deployment of a dedicated sensor network.
 - Insights are easily accessible for authorized users, enabling them to quickly retrieve critical information. This rapid access to data can fast-track investigation cases and support timely decision-making in various operational contexts.
- **Leads to cost savings and operational efficiencies:**
 - With a fully integrated cloud-based architecture, governments, telecom regulatory agencies, and MNOs can collaborate to reduce licensing costs, scale solutions efficiently over time, and significantly enhance security and monitoring capabilities at a national scale.
- **Unlocks a wide range of use cases:**
 - For governments, mobile network intelligence can support emergency services, public risk detection, and emergency call location.
 - For MNOs, compliance with regulatory requirements and the monetization of data through network APIs present new business opportunities.

By harnessing mobile network intelligence, governments can significantly enhance their national security efforts, tackle emerging threats more effectively, and do so in a way that respects individual rights and complies with legal frameworks. The future of homeland security lies in the innovative application of mobile network metadata and intelligent analytics, and there's no reason to wait: the technology exists and experience has proven its efficient use, all over the world.



Intersec is a global leader in telecom metadata and location intelligence solutions. Designed by fast data experts, our solutions guide governments and telcos in their data-driven revolution to build tangible value, from efficiently warning people in case of danger to driving new sources of revenue. Our 90 clients in 40 countries leverage our instruments to reach, locate, and map nearly one billion connected devices 24/7, and our mission-critical communication solutions cover 400 million people around the world. Headquartered in France, Intersec places Privacy by Design well beyond accepted standards, it assures regulatory compliance, no matter where our clients operate. Learn more at intersec.com.

