POSITION PAPER

Digital Networks Act

Public Warning Systems, Emergency Call Location & Homeland Security

Intersec — Response to the European Commission Consultation — June 2026

Table of contents

Contact

Charlotte Cardona - Public Affairs

charlotte.cardona@intersec.com - +33 (0)6 74 39 12 93

Executive summary

Intersec welcomes the Digital Networks Act (DNA) as a timely and necessary step towards a more harmonised, resilient and competitive European digital infrastructure. As a French technology company specialising in network-based geolocation and public safety solutions deployed in over 50 countries and serving 1 billion people globally, Intersec brings unique operational expertise to this consultation.

Intersec has a complete offering spanning the entire chain, from mobile networks to the end-user applications used by civil protection authorities and emergency services. This gives us a complete view not only of the capabilities offered by mobile networks, but also of the needs of end users. And this across the world. We wish to make this knowledge and expertise available to contribute to and help make the DNA as useful as possible for EU Member States and their populations.

This position paper focuses specifically on Articles 5, 106 and 107 of the Proposal for a regulation of the European Parliament and of the Council on Digital Networks which governs emergency caller location and public warning systems, and which the DNA largely carries forward. We argue that the DNA presents a critical window of opportunity to correct longstanding implementation failures and close dangerous gaps in the protection of EU residents.

Our core recommendations are:

- Mandate Cell Broadcast as the universal channel for immediate population-wide alerts, with device pre-configuration and activation as a condition of market access in the EU.
- Mandate a persistent messaging channel (location- or registration-based SMS and/or mobile application) for non-urgent, informational alerts alongside Cell Broadcast.
- Mandate real-time aggregated population density reporting by mobile network operators to support crisis situational awareness.
- Mandate real-time network readiness reporting for public safety functions (typically alert broadcast, emergency calls management).
- Mandate combined use of network-based and handset-derived (AML) location for all emergency calls, with binding accuracy of 50m for 80% of calls.
- Require all device manufacturers selling in the EU to enable device support, configuration and activation of AML as well as all relevant 3GPP geolocation primitives.
- Mandate cell-level and sub-cell active geolocation on all EU mobile networks for homeland security purposes, with passive geolocation data retained for a minimum of 3 months.

Our recommendations are structured across three levels of priority, colour-coded throughout this paper:

- **Mandatory** (red): binding obligations that must be inscribed in the DNA text
- **Recommended** (orange): measures that Member States should be strongly encouraged to adopt
- **Optional** (beige): additional capabilities that bring operational value and whose activation is encouraged where feasible.

About Intersec

Intersec is a French software company founded in 2004 and a recognised European leader in telecom metadata, location intelligence, and public safety applications. Our technology combines mobile network positioning (2G–5G) with handset-derived location (Advanced Mobile Location, or AML) to deliver the highest possible accuracy and reliability for emergency services.

Intersec serves both mobile network operators and public authorities, a dual perspective that gives us a uniquely informed view of this policy space: we understand network capabilities and implementation constraints from the inside, while directly capturing the operational requirements of the agencies and governments that depend on them.

Our credentials in the public warning and emergency location space speak for themselves:

- Cloud-native solutions deployed in 50+ countries, locating over 1 billion connected devices worldwide.
- 47 civil protection systems deployed across Europe, the Middle East, Africa, Asia-Pacific and Latin America, protecting 460 million people worldwide.
- 31% global market share in Public Warning Systems (17 out of 60 equipped countries), with 70% year-on-year growth.

Our subject-matter experts have accompanied deployments across all major positioning technologies, accumulating field experience - particularly in the Middle East, where customers have deployed the full range of available technologies to ensure the widest coverage, finest accuracy and guaranteed reliability - that directly informs the recommendations set out in this paper.

I. Recommendations for Public Warning Systems

The requirements below are grounded in operational feedback from civil protection authorities and duty officers across Intersec's 47 deployments worldwide, and reflect lessons learned from managing real crisis situations.

1.1. Efficient alert dissemination

The objective here is to send a message with instructions and directions to the population as efficiently as possible, adapted to the nature of the alert. To this end, several channels are available:

- Mobile phones: network technologies (Cell Broadcast, Location-Based SMS depending on the mobile phone location or on registered address), and smartphone applications.
- Traditional channels: sirens, highway signage panels, television, radio, urban display panels.
- Digital channels: social media, emails, institutional web portals.
- Emerging channels: satellites, EU Wallet

R1

Mandate Cell Broadcast as the universal immediate-alert channel

In our view, it is necessary to activate a channel that enables instant dissemination to a large population, and if needed to the entire population of a country. This channel is typically required for immediate or imminent alerts: meteorological threats, violent storms, flooding, aerial threats, security incidents. The appropriate channel for this type of alert is Cell Broadcast. This requires:

- **Network activation:** activation of the corresponding capabilities on relevant mobile network equipment.
- **Device pre-configuration:** all mobile device manufacturers selling on European territory must ensure that their devices are pre-configured to receive alerts issued by any mobile network of the European Union, as well as EEA countries, Balkans countries, Ukraine, and other EU membership candidate countries. This must not depend on device initialisation, registration on a manufacturer platform, or on the one of the operating system.

It is also observed that this channel is already very widely implemented across EU Member States (~85%); only a few States are not yet equipped. This is a recommendation also made by EENA, which notes the increasingly systematic adoption of this proven technology.

R2

Mandate a persistent messaging channel alongside Cell Broadcast

In our view, it is necessary to activate a second channel that enables dissemination of informational messages which, unlike Cell Broadcast, will persist on recipients' devices. The purpose is to cover alert types that are not necessarily urgent, but where recipients need to be able to refer back to the information after receiving it. For example: flood risk in the next four days, reminders of the conduct to follow, and information on which media to consult to stay informed.

Such a channel must provide the following capabilities:

- **Persistence**: received messages must be persistent, allowing the user to refer back to them later, or to forward information and recommendations to third parties and family members.
- **Multimedia content**: messages must be capable of carrying multimedia content, supporting inclusivity and providing more readable information and directions to the population.

Two channels enable such dissemination, and we believe each Member State should decide which is most appropriate for its local context:

- **SMS** (based on the current location of the mobile device or on registered address): SMS messages are received and stored on the mobile device. Users can forward them. They can contain a link to a website with instructions in multimedia format. On this subject, Intersec notes that a misconception is circulating: a number of deployments of this channel have been criticised as insufficiently effective in message distribution because the volume of SMS would saturate mobile networks. These

shortcomings are inherent to the insufficiently performant technology of certain platform providers. We have demonstrated - in France, in Croatia and elsewhere - that it is not only technically possible to send tens of thousands of SMS instantaneously, but that crisis management teams benefit from such essential operational instruments.

- **Mobile application**: provides the best user experience. It enables multimedia content dissemination to provide instructions in visual form using maps, synoptic displays, and video instructions. This enables inclusivity: reaching illiterate populations and overcoming language barriers by offering universal visual content. It also enables two-way communication, triggering interaction with alerted populations or collecting feedback from them. However, it requires installation by the user (or pre-installation by the device manufacturer) and is therefore not available by default on all devices as SMS is.

R3

Mandate Galileo satellite alert channel by Jan. 2030, obligatory by 2033

Intersec recommends activation of the Galileo satellite channel by January 2030, and recommends making it obligatory by 2033, once the installed base of mobile devices supporting this channel has reached a critical size. This channel is necessary to ensure alert dissemination in white zones, or to extend reach across borders when sending an alert, whether those gaps are permanent (areas not covered by the mobile network) or temporary, caused by the disaster itself (damaged or destroyed sites and antennas).

It should be noted that the Galileo channel is not a substitute for the use of terrestrial networks for sending alert messages. Even though it provides global geographic coverage, it presents several limitations:

- It is not supported by all mobile devices.
- It only allows the transmission of pre-determined messages from a hard-coded list.

R4

Enable registration-based alerting for personalised notifications, independent of the device's current location

A registration-based channel allows citizens to subscribe and define areas of interest for receiving alerts - for example, the address of a secondary residence, or the location of an isolated family member. Email, SMS or mobile application channels can all be used to handle such alert messages, informing those who wish to receive them.

For example, Intersec contributed to the new flood warning system in England, which now has over 2.6 million registered users, and this number continues to grow because personalised alerts help to avoid “alert fatigue” and contribute to risk awareness culture.

R5	**Establish an EU-wide alert database for cross-border notification continuity** Intersec recommends the creation of an EU database in which each Member State can post a copy of the alerts it sends. National smartphone alert applications could then, when a user travels to another country in the Union, continue to display certified content made available by the local government.

R6	**Leverage traditional and digital channels as complementary dissemination layers** Traditional channels (television, radio, sirens, highway signage) and digital channels (social media, institutional web portals) can usefully complement the channels described above. Their activation is encouraged but should be treated as optional within the DNA framework, given the inherent limitations of each in terms of geographic precision, real-time reach and universal availability.

1.2. Situational awareness

The first requirement for effective crisis management is having the most accurate information reported from the field, in real-time. In this domain, mobile networks provide two key components.

- **Network availability for alert dissemination:** Is the network fully capable of broadcasting alerts, or only partially so? Before launching an alert over a defined perimeter, it is important to know whether the corresponding antennas are operational, or whether they may have been damaged by the very event about which an alert is to be issued.
- **Population density**: How many people will be alerted? This information is useful for determining the scale of the alert in advance and estimating the expected impact of sending an alert. After the initial alert - which may for example contain evacuation instructions - it is useful to see population density evolve to understand whether the population is able to follow the instructions, or whether it may be useful to send emergency personnel to relay instructions or facilitate evacuation.

R7	**Provide real-time aggregated population density data** Mobile networks should ideally provide an aggregated data feed - meaning a population count, not the individual location of mobile subscribers - allowing a consolidated representation of population density across the country to be built and reported in real time to crisis managers.

R8	**Provide a real-time network state feed for alert broadcast capability** Mobile networks should ideally provide a real-time feed presenting the state of the network - that is, its capacity to send alert messages - in the form of a coverage map with the positions of antennas, their orientation and emission radius, as well as an on/off status for each antenna and the number of subscribers currently connected to it. Beyond uses related to alerting, this also allows crisis managers to understand whether telecommunications are functioning correctly in any given location.

R9	**Report locations with high concentrations of emergency calls** Reporting of locations with high concentrations of emergency calls would allow authorities to identify and confirm in real time whether a specific location may require attention.

II. Recommendations for Emergency Call Location

2.1. State of play

- **270 million emergency calls per year in the EU**
- **~800 lives that could be saved annually with better location**
- **10% of calls received with NO location information**
- **€55–100 billion potential net benefit over 10 years**

Sources: EC 2024 report on EU emergency number 112 ; HELP112 II project (EC-funded) ; EENA

A legal obligation that exists on paper

Article 109 of the EECC (Directive - 2018/1972) requires Member States to establish criteria for the accuracy and reliability of caller location information, combining both network-based and handset-derived technologies. The compliance deadline was 5 March 2024.

> *"In the case of an emergency, the location of the caller is the most important piece of information for emergency services. Not having it will mean longer calls to understand the position of the victim, delayed arrivals of rescuers at the scene, a shortage of ambulances and sometimes fatal consequences."*
>
> — HELP112 II Project, European Commission (D4.2)

Mass non-compliance by Member States

Despite the 5 March 2024 deadline, the vast majority of Member States have not published the required criteria for caller location accuracy and reliability. Only a handful - including Bulgaria, Germany and Greece - have issued a formal decision or regulation.

BEREC confirmed in December 2024 that existing EU guidance was “insufficient,” leading to inconsistent implementation, and recommended that clear criteria be set at EU level. EENA’s 2025 response to the DNA call for evidence echoed these concerns, noting that handset-derived caller location “still suffers from several drawbacks which inhibits its effectiveness.”

A sovereignty risk: EU citizens’ lives depend on US platform decisions

Apple and Google together hold ~100% of the EU smartphone market (38–39% iOS, 61–62% Android). Advanced Mobile Location (AML), the current protocol for transmitting handset-derived caller location, depends entirely on these two vendors choosing to keep it enabled, with no EU regulatory requirement to do so.

This is not a theoretical risk. In January 2026, Apple quietly rolled out a security feature limiting mobile networks' ability to collect precise location data from iPhones, complicating law enforcement access to caller location. If Apple or Google were to restrict or disable AML - for privacy, commercial, or geopolitical reasons - emergency caller location across the entire EU would be compromised overnight. This need not even be a deliberate, AML-specific decision: a broader platform update or geopolitical disruption could have the same effect. The root issue is structural: EU residents' safety depends on services controlled by two US corporations, with no EU regulatory safeguard in place.

2.2. The role of location in emergency call handling

Emergency caller location enables above all an **efficient handling of each call**, by automatically providing context information about the call. The call taker gains certainty when interacting with the caller, who may be disoriented or under stress, and does not need to ask the person in distress to communicate their position (assuming they are even able to do so). This saves time in call handling and enables faster dispatch of emergency services or in some cases, the detection of fraudulent calls, where a person reports events while being several hundred kilometres away from where the events are alleged to have occurred.

The precision of geolocation is essential to derive an address to which emergency services can be dispatched.

The value of geolocation for emergency call management is not only measured through the spatial dimension but also through the temporal one. It unfolds across three distinct phases:

- The location of the call must be instantly available at call establishment: this information will be used to route the call to the nearest emergency call centre. Note that for this purpose, the location does not need to be known with great precision.
- In a second phase, when the call is answered, the caller’s geolocation must be provided with a level of precision that allows emergency services to be sent to an address. Obtaining this precise location may require some time, depending on the geolocation techniques deployed at network level and by the mobile device operating system (AML). During this phase, multiple locations may be transmitted to the emergency call

centre, reflecting either a progressive improvement in precision or a movement by the caller.
- Then throughout the call, new geolocation points must be obtained — for example, to correctly handle cases such as abductions.

Today, Article 109 of the EECC (Directive - 2018/1972) requires combining device-derived geolocation (AML) and network-derived geolocation and establishing precision criteria before 5 March 2024, but most EU countries are slow to define these criteria and to require them of operators.

2.3. Combined network-based and handset-derived location

R10	**Mandate combined use of network-based and AML location for all emergency calls** The geolocation of an emergency call must rely on both network-derived geolocation and device operating system-derived geolocation (AML). Network-derived location cannot be spoofed, and is in no way dependent on the terminal, which may be subject to the goodwill of the OS provider.

R11	**Mandate 50m accuracy for 80% of emergency calls** Sub-cell geolocation must be activated to guarantee 50m precision for 80% of emergency calls across the entire EU territory (per EENA's recommendation).

2.4. Network-based geolocation: technical framework

Emergency call network-based location is defined by 3GPP/OMA standards, which standardise over 30 different geolocation techniques. No single location technique provides optimal performance in all environments. Each technique has inherent strengths and limitations:

- **A-GNSS**: delivers high accuracy outdoors but fails indoors.
- **Timing-based techniques** (such as Time Difference of Arrival — TDOA): perform well in rural areas with clear line-of-sight to cell towers but degrade in densely populated urban environments due to multipath interference and signal reflections off building facades.
- **RF Fingerprinting**: provides the highest precision in all environments but requires regular drive tests to maintain the quality of the signature database, resulting in higher operational costs.

Based on Intersec's experience deploying location technologies across more than 50 countries, combining multiple techniques - triggering them simultaneously or sequentially and selecting the best available result for each call - delivers significantly better results than relying on a single method.

However, it belongs to each Member State, in consultation with its national mobile operators, to determine which techniques are relevant, based on its own criteria (mobile network density

relative to geography, etc.). The same techniques will not be implemented in a very dense country such as Luxembourg as in a large country such as France, Spain or Germany. Moreover, the implementation cost of the different techniques varies across network generations, the right compromise between investment and results must be found.

Since activating all techniques is not reasonable, Intersec recommends the following approach:

R12	**Mandate cell-level location as the universal baseline** Cell-level geolocation must be systematically activated. This geolocation is available instantly at call establishment. Its spatial precision depends on location and is proportional to population density: it can reach 200m in dense urban areas and 10km or more in sparsely covered rural areas. This geolocation enables routing of the emergency call to the nearest Public Safety Answering Point (PSAP) (where this is the model in use in the country) and provides a low-cost coarse location of the caller.

R13	**Mandate sub-cell location** Sub-cell geolocation must be activated to guarantee 50m precision for 80% of emergency calls (per EENA's recommendation). Intersec's recommended approach is to allow each Member State to work with its mobile operators to select at least one sub-cell geolocation technique per network generation. This also provides a level of resilience should AML support ever fail or be withdrawn.

R14	**Activate RF Fingerprinting for highest-accuracy zones** Intersec recommends activation of RF Fingerprinting techniques to achieve the best geolocation precision. As this technique carries an operational cost to maintain the quality of the signature database, it may be activated only in certain areas to optimise the cost-benefit ratio - for example in high-density urban areas.

2.5. Handset-derived location (AML)

R15	**Mandate AML activation for all devices sold in the EU** Handset-derived location (AML) must be activated and configured for all compatible terminals sold on the territory of the European Union. On each device sold in the Union, the short code SMS and HTTPS transmission URLs for all countries of the Union must be configured and provisioned. Extending this to a few additional countries (UK, EEA, etc.) is also relevant, as emergencies do not stop at borders. Furthermore, at the mobile network level, these SMS and HTTPS requests must be routed to AML platforms at no cost, bypassing the operator's billing system.

III. Recommendations for Homeland Security

In the face of growing external threats to EU Member States and internal security threats, it is essential that the police forces and security services of EU Member States are equipped with effective tools in the fight against crime and security threats.

At a time when all communications are becoming encrypted (up to 95%) and Member States are becoming aware of the risks associated with intrusive investigation solutions (cf. data privacy), cyberattacks and foreign interference threats, telecom metadata - or connection data - is becoming an undeniable, incontestable and non-intrusive source, increasingly favoured by investigators, all the more so as technological advances now allow, through processing this data, to derive exceptional and unique intelligence, accelerate investigation timelines and, at the same time, optimise the management of their public policies.

To this end, it is essential that police forces and government agencies in EU Member States have access to this metadata, in particular geolocation data. Intersec recommends several levels of performance, from the minimum to the most sophisticated.

This geolocation data comes in several forms:

- **Active geolocation**: enables on-demand computation by the network of the location of a device containing a SIM card, with cell-level or sub-cell precision. It relies on standards defined by 3GPP and OMA.
- **Passive geolocation**: consists of collecting the geolocation of devices containing SIM cards as it is carried within mobile networks to ensure their proper functioning.

These two approaches to mobile network geolocation provide complementary benefits in the context of law enforcement and security services.

3.1. Active geolocation

R16

Mandate cell-level active geolocation on all EU mobile networks

Cell-level active geolocation must be systematically activated on mobile networks. Intersec estimates that to date, approximately 80% of EU mobile networks have activated this capability.

R17

Mandate sub-cell active geolocation and device-level 3GPP support

Intersec's recommended approach is to allow each mobile operator to select at least one sub-cell geolocation technique per network generation. Furthermore, device manufacturers selling in the European Union must be required to ensure that their devices support the protocol primitives related to geolocation functions (for example, activation via the LPP interface of the terminal's GPS positioning by the network – cf. 3GPP TS 37.355).

R18	**Activate RF Fingerprinting for highest-accuracy requirements** Intersec recommends activation of RF Fingerprinting techniques to achieve the best geolocation precision. As this technique carries an operational cost to maintain the quality of the signature database, it may be activated only in certain areas to optimise the cost-benefit ratio, for example in high-density urban areas.

3.2. Passive geolocation

R19	**Mandate passive cell-level geolocation and minimum data retention of three (3) months** This type of geolocation consists of capturing geolocation data as it circulates within mobile networks. It is indispensable to "find a needle in a haystack", support pattern detection, both in real time and retrospectively. Our recommendation is consistent with the findings of the EU High-Level Group (HLG) on access to data for effective law enforcement. Intersec recommends a retention period of a minimum of 3 months, extendable up to 36 months.

R20	**Enable passive sub-cell geolocation for high-priority security operations** Passive sub-cell geolocation is very useful for detecting individuals involved in serious criminal activity, terrorism and foreign interference attempts. The use of passive sub-cell geolocation allows security services to obtain results that could not otherwise be achieved: in border surveillance - particularly at the EU's external borders - in surveillance of strategic locations on national territory (military bases, energy production sites, critical industries), and in other high-priority security operations.

On Regulatory Harmonisation: Responding to BEREC

BEREC has expressed concern that the DNA, in its current form, may not sufficiently ensure effective national enforcement, and advocates for maintaining national flexibility where EU rules remain insufficiently detailed. Intersec notes these concerns regarding legal continuity and the risk of regulatory gaps during transition.

On the specific question of emergency communications, however, Intersec's position diverges. The implementation record of the EECC provides a clear natural experiment. Article 110 — which imposed a binding obligation on Member States to deploy mobile-based public warning systems (Cell Broadcast and/or Location-Based SMS) by June 2022 — has, despite initial delays, driven near-universal deployment across the EU. The binding nature of the obligation,

and the prospect of infringement proceedings, ultimately produced results. Today, the majority of Member States are equipped.

Article 109, by contrast, left the definition of accuracy criteria for emergency caller location to Member States, with no binding precision requirements at EU level. The result: seven years after the EECC entered into force, the vast majority of Member States have still not published the required criteria. The non-binding nature of this obligation has produced exactly the fragmentation and inaction that the DNA now has an opportunity to correct.

Intersec therefore calls on the DNA to set harmonised, binding and operationally precise requirements for emergency caller location and public warning, not as a ceiling, but as a floor. Member States that wish to exceed these standards should remain entirely free to do so. But every EU citizen, regardless of where they live or travel, must be guaranteed the same minimum level of protection. This is precisely what a Regulation makes possible, and it is an opportunity the DNA must not forfeit.

Intersec calls on the European Commission and co-legislators to use the DNA to address these gaps decisively.

Conclusion

The Digital Networks Act arrives at a pivotal moment. The EECC created the right obligations; the DNA must now create the enforcement architecture to make them real. Emergency caller location and public warning are not technical niceties, they are foundational services that EU residents depend on in the most critical moments of their lives. An estimated 800 lives per year could be saved with better location accuracy. The economic net benefit has been estimated at between €55 and €100 billion over ten years. The cost of inaction is measured in lives.

Intersec calls on the European Parliament and Council to use the DNA to:

- Set binding, harmonised and operationally precise requirements for emergency caller location, public warning and homeland security geolocation capabilities, not as a ceiling, but as a floor.
- Mandate Cell Broadcast pre-configuration, AML support and 3GPP network primitive compliance for all devices sold in the EU.
- Require real-time network readiness and aggregated population density reporting to enable effective crisis management.
- Clarify that mobile applications are a complementary bearer only, never a replacement for network-based emergency communications.
- Mandate passive geolocation data retention to provide law enforcement agencies with the operational tools they need.

Europe cannot afford to leave the safety of its residents dependent on the voluntary goodwill of foreign platform vendors. The DNA is the opportunity to change this. Intersec stands ready to provide technical expertise to legislators and regulators in support of these objectives.