EuroISPA reaction to the 42 Recommendations of the High-Level Group on Access to Data for Effective Law Enforcement

EuroISPA, the world's largest association of Internet Services Providers (ISPs), representing over 3300 ISPs across the EU and EFTA countries, welcomes the work and efforts of the High-Level Group (HLG) on access to data for effective law enforcement on promoting a high level of security and an effective approach to fighting crime and other challenges through the proposed 42 Recommendations.

In anticipation of the upcoming discussions of the HLG in the autumn, and as suggested by the experts of the group, EuroISPA would like to take this opportunity to react and give constructive feedback to the recommendations, highlighting some elements that require a careful approach besides further thinking.

In particular, EuroISPA is concerned with some proposed recommendations that could weaken encryption, which is a fundamental tool to protect European citizens' fundamental right to privacy. Moreover, we underline the need to carefully assess any further measures that can put more burden on European actors, especially the smallest ones. Finally, any additional measures should take into account the complex value chain that characterises the different ECSs (Electronic Communications Services); any unclear measure might lead to loopholes, further uncertainty when conducting business, as well as threats to the security and the integrity of networks.

Recommendation 10 on cooperating with Electronic Communications Services to develop a methodology for lawful access measures when access to data is not possible

Although clarified that those cases should remain exceptional and that law enforcement authorities should only make use of such tools as a last resort, it is imperative that all access demands are implemented solely by the relevant ECS provider upon receipt of appropriate legal documentation. This will ensure security, privacy and integrity of networks.

Recommendation 17 on fostering transparency rules for ECS providers

Any transparency rules or new obligations must be proportionate and take carefully into consideration the different business capacity of ECSs. On lawful interception obligations for judicial purposes, we stress once again the importance of respecting the secrecy and confidentiality of the investigation.

EuroISPA
Rue de la Loi 38, 1000 Brussels
secretariat@euroispa.org
EU Transparency Register: 54437813115-56

Recommendation 22 on implementing a lawful access by design in all relevant technologies in line with the needs expressed by law enforcement, through the development of a technology roadmap

Although we support the idea of a technology roadmap, the purpose should not result in a lawful access by design, which EuroISPA opposes firmly.

Recommendation 23 on ensuring that new obligations, new legal instruments or standards do not weaken E2EE

EuroISPA invites the HLG to keep in mind and be consistent with this consideration. Despite agreeing that any new rules should avoid any weakening of E2EE, EuroISPA urges to be careful in considering access to data in clear, as it will intrinsically weaken what was intended to be encrypted in the first place.

Recommendation 27 on establishing a harmonised EU regime on data retention

The ability to "provide access" should not be an element to consider when defining the scope of the providers obliged to respond to an order. EuroISPA defends a cascade approach and access closer to the source, as so to avoid unfair requests and indiscriminate targeting.

We are against any measures that will weaken encryption or create backdoors, as weakening encryption and cyber protection exposes citizens and businesses to crime, besides putting in danger infrastructure from foreign attack.

Furthermore, there are no solutions that allow the decryption of encrypted data without compromising its integrity and security and any claims affirming the opposite will be putting in danger the EU efforts to increase the level of cybersecurity across the Union (i.e. NIS2, CER, etc.).

Therefore, any obligations to ensure this access should remove providers from any liability for issues derived from its exploitation by malicious actors.

Finally, the list of data categories that have to be retained on a mandatory basis should be only data already processed and stored for billing, commercial, technical, security or other legitimate purposes. The conditions for ordering the retention of data should vary according to the data category concerned. Any further request in this sense would be disproportionate and contrary to the principles of data minimisation and fundamental rights.

Recommendation 28 on categorising data on the basis of its purpose and Recommendation 29 on ensuring that access to data is targeted and differentiated

It should be clarified who will be in the scope of such obligations, as classifying information in a preventively way would put extra red tape on companies.

EuroISPA reminds that classifying data for enforcement purposes and not business purposes is not a task of services providers.

Recommendation 30 on including rules on accountability and enforceability for service providers in order to enforce obligations to retain and provide data

EuroISPA suggests a careful approach, as ECS providers must be able to store the data securely and organise this process in the most efficient and effective way to their operations. Moreover, future EU legislation should be focused on providing clear objective criteria to define the specific circumstances and conditions under which a service provider in scope must retain individual users' data for the purpose of granting access to LEAs, and jump on accountability and enforceability measures only if necessary.

Recommendation 31 on making sure that user data retained for commercial and business purposes is accessible for law enforcement under relevant safeguards

There is no legal basis and lack of objective criteria to justify LEAs access to any data and for any purpose when the data has been stored for business purposes. Data should only be available to fulfil requests linked to serious crimes. Any other approach will create issues linked to liability and retention periods.

Recommendation 32 on obligations on service providers to turn on or turn off certain functions in their services to obtain certain information after receiving a warrant

This creates a proactive role for providers to "spy" their users (direct surveillance). Moreover, providers should not be obliged to respond to LEAs' requests in instances where LEAs have no authorisation on; providers should not become a backdoor for authorisation procedures.

Moreover, we can foresee issues linked to proportionality, technical limitations, costs and privacy.

Recommendation 33 on sanctions against non-cooperative Electronic Communications Services (including harmonisation of imprisonment as in Recommendation 34)

This creates huge legal uncertainty as there is no certainty[1] on how non-cooperation or deliberate action is defined. Any application of criminal law should be based solely on the ruling of a judicial authority.

Moreover, There are limits to the harmonisation of criminal law. This might also create issues with existing legislation as the DSA.

Recommendation 37 on subject providers of Electronic Communications Services (as defined in the EECC) to the same rules as traditional service providers

Subjecting ECSs to the same rules as traditional service providers might disrupt the level playing field, creating disproportionate obligations; obligations should be relevant to the specific services provided by ECSs, which is what differentiate them from traditional service providers in the first place. This should be carefully assessed keeping in mind especially European SMEs.

[1] The footnote trying to better define 'non-cooperative ECSs' reads that: 'In that context, Non-cooperative Electronic communications Services is defined as any operator who does not comply with legal orders and requests of a technical nature addressed by the law enforcement and has no objective reason for doing so.'

Recommendation 38 on further harmonising national legal frameworks for access to data in transit

Widening the scope adds legal uncertainty for providers that should not be naturally targeted by LEAs' requests in this space.

Same as with encryption, the creation of backdoors for any purpose does not only create privacy and proportionality issues but also cybersecurity concerns, as this access could be exploited by malicious actors (cybercriminals and foreign state actors), making the EU an easy target for cyber criminals.

Moreover, see Recommendation 41 noting that "[…] measures should not imply an obligation for providers to adjust their ICT systems in a way that negatively impacts the cybersecurity of their users."

Recommendation 39 on adjusting the concept of territorial jurisdiction over data to address potential conflicts of laws with other jurisdictions

Approach to territoriality cannot be adjusted on a case by case basis: there has to be a rule that is well known and consistent. As we understand, an approach as suggested in Recommendation 39 would be dangerous and requires further clarification.

About EuroISPA

Established in 1997, EuroISPA is the world's largest association of Internet Services Providers Associations, representing over 3,300 Internet Service Providers (ISPs) across the EU and EFTA countries. EuroISPA is recognised as the voice of the EU ISP industry, reflecting the views of ISPs of all sizes from across its member base.

EuroISPA
Rue de la Loi 38, 1000 Brussels
secretariat@euroispa.org
EU Transparency Register: 54437813115-56