
Public consultation on improving cross-border access to electronic evidence in criminal matters

EuroISPA accompanying position paper

Introduction

EuroISPA¹ is the voice of the European Internet industry, representing over 2500 Internet services providers from across the EU and all along the Internet value chain.

EuroISPA and its members welcome the opportunity to provide input into the European Commission's reflections on how to improve the fight against cybercrime.¹ Indeed, many of the companies represented within EuroISPA – including access providers, hosting providers, domain name registries, and hotlines – have worked with law enforcement (LE) and judicial authorities² in their countries of operation for many years, and thus have valuable insights on the functioning of existing cooperation frameworks between the various parties, and how they could be improved. Moreover, the overwhelming majority of companies represented in EuroISPA are classified as small- and medium-sized enterprises, and as such, face novel challenges from any new legal regime that places new compliance burdens upon private actors.

In the below section, EuroISPA will seek to outline the principles that underlie its consultation response, and the motivation for such.

ISPs should only deal with national judicial and law enforcement authorities

Since their founding in the mid-1990s, the national associations of Internet service providers represented in EuroISPA have worked hard to develop trust and effective cooperation with their national LE and judicial authorities. The endeavours made by both sides have proven extremely fruitful, with many companies represented within EuroISPA reporting highly efficient cooperation procedures for receiving and acting upon LE/judicial authorities' requests for data and facilitating criminal investigations generally.

The trust and respect that underpins the effective cooperation between Internet service providers and their national LE/judicial authorities owes itself predominately to the unique and special relationship that exists between the state and the natural/legal persons that comprise it. This relationship is embedded in broader

¹ EuroISPA regrets that the design of the European Commission's online consultation tool was such that not all relevant questions were made available to specific categories of respondents. Given the importance of the consultation and EuroISPA's representative role for several categories of service providers, the association has submitted three separate consultation responses: (1) interest group; (2) information society service provider; (3) electronic communication service provider.

² In this paper, the generic term 'public authorities' is used when speaking of law enforcement and judicial authorities as a collective.

political, social, and cultural factors, and must remain a key consideration when assessing optimal frameworks for LE/judicial authorities' cooperation with ISPs.

Yet there are also more material considerations that determine the effectiveness of cooperation between public authorities and service providers, and which suggest that cross-border direct cooperation is unsuitable:

- Most importantly, ISPs can (without much difficulty) verify whether a request from a national public authority to access data is authentic and whether the authority in question is empowered to request such data. Conversely, ISPs face huge difficulty in verifying the authenticity of another country's law enforcement agencies, and whether they have the authority even in their own country to demand the information they are seeking.
- Moreover, ISPs operating in a country will almost certainly be able to interact with their national LE/judicial authorities in a shared language. This would not be the case with respect to foreign law enforcement, and a move towards direct cooperation would suggest that ISPs would need to translate legal requests and statutes from other jurisdictions, and extremely costly and time-consuming process.

On the above basis, EuroISPA and its members assert that ISPs should only deal with national LE/judicial authorities. The Mutual Legal Assistance (MLA) procedure and the new European Investigation Order (EIO), as well as the recently-created European Public Prosecutor Office provide ample tools for EU and public authorities to carry on their investigation both in the digital and physical domain. These mechanisms alleviate the cooperation problems mentioned above, in virtue of the crucial fact that an ISP is only required to cooperate with public authorities in its *home country* under those frameworks.

A legal framework that seeks to enhance the effectiveness of cross-border digital investigations by breaking the cooperation link between an ISP and the public authorities in its home countries will have the opposite outcome – slower access to data, and more legal uncertainty.

Any new compliance obligations should be off-set by effective cost-reimbursement regime

As noted above, the overwhelming majority of ISPs represented in EuroISPA are small- and medium-sized enterprises. Many of these enterprises operate on tight margins, and depend on agility and resource efficiency to compete against the much larger incumbent and multinational service providers. In that context, any additional compliance burden threatens these companies and their ability to compete on the market.

The obligation to cooperate directly with public authorities located in foreign countries would place considerable additional fixed and marginal costs on SME ISPs. Such ISPs would be forced to undertake capital investment in new mechanisms for handling cross-border requests for data (e.g. secure communication channels, dedicated staff), and would also be forced to devote more resources to deal with the unique challenges that arise from direct cross-border requests (e.g. translation costs, assessment of legal basis, etc).

In recognition of the considerable compliance costs from ISPs whenever they cooperate with law enforcement - and the disproportionate impact of this on smaller operators – many EU Member States include specific mechanisms of compliance cost reimbursement for ISPs within their national legal codes. While there is

considerable divergence in the effectiveness of these mechanisms across Member States, the principle is sound. Indeed, any new framework that foresees ISPs directly cooperating with public authorities in foreign countries would need to replicate this principle, by including a cost reimbursement mechanism at its core. Besides the economic rationale, this would have an added bonus of disincentivising public authorities from sending frivolous or bad faith requests for data.

Without a meaningful cost reimbursement mechanism, direct cooperation regimes would put SME ISPs at a clear market disadvantage, with serious consequences for economic growth and competition in many EU Member States.

Conclusion

EuroISPA has been a longstanding interlocuter in policy discussions on how to improve cooperation procedures, and has used its representative role at – amongst others – Europol's EC3 communications providers advisory group, the European Commission DG JUST/DG HOME taskforce on e-evidence, and the former European Commission expert group on data retention, to advance those discussions.

It is on the basis of this experience that EuroISPA and its members feel compelled to stress the negative consequences that will arise from any framework that forces ISPs to cooperate directly with foreign law enforcement. We also highlight that these problems can be avoided by effective implementation of the new European investigation order and the European Public Prosecutors Office, as well as a meaningful effort to reform MLA procedures between national public authorities.

EuroISPA looks forward to providing additional input to the European Commission's reflections on these important matters.

About EuroISPA:

EuroISPA is the world's largest association of Internet Services Providers (ISPs) representing the interests of more than 2500 Internet infrastructure companies across the EU and the EFTA countries. EuroISPA is a major voice of the Internet industry on information society subjects such as cybercrime, data protection, e-commerce regulation, EU telecommunications law and safe use of the Internet. Contact: Secretariat (+32 2 550.41.14/ secretariat@euroispa.org)