VERBAND DER INTERNETWIRTSCHAFT E.V.

STATEMENT

On the European Commission's Call for Evidence Without an Impact Assessment on the European Internal Security Strategy (Ref. Ares (2025)1157428 - 13/02/2025)

Berlin, 13 March 2025

The European Commission has set out to develop a new European Internal Security Strategy and has launched a consultation on the topic. The new Internal Security Strategy is intended to further explore challenges arising from a "global and interconnected environment in which criminal networks, terrorists, extremist groups and hostile state and non-state actors operate, both within and beyond the EU" and presumes the necessity for further action against the threats identified. The assumption includes the assessment that "digital technology will play a substantial role in the Strategy". According to the plan, this includes data access for law enforcement, data retention and cooperation with tech platforms among other measures.

eco – Association of the Internet Industry would comment on the topics raised by the Commission as follows:

- **Measures on access to data for law enforcement**

With the European e-Evidence Package ((EU) 2023/1543 and (EU) 2023/1544), new measures for the lawful obtainment of information by criminal authorities were created in 2023, supplementing the existing system of Mutual Legal Assistance Treaties (MLATs) and partially supplanting them. This legislation is currently in the process of being implemented in the respective Member States. The necessity for creating new measures or reforming existing ones is not comprehensible. Every reform of existing legislation requires companies in the Internet Industry to invest in further compliance, diminishing their turnovers and creating legal uncertainty with regards to the correct implementation as well as the coherence with fundamental and consumer rights. From the point of view of the industry, it is imperative, that the legislation which has only been put in place needs proper implementation and evaluation before further legislative or regulatory activity is undertaken.

Additionally, the topic by itself raises the question in how far the "access to data" element is interpreted by the Commission. If the topic explores the idea of undermining end-to-end encryption through any means, eco would like to recall that any attack on encryption, whether through lowering crypto-complexity or providing side channels for accessing encrypted information is ultimately an attack on cybersecurity, undermining the trust in digital technologies and constituting an

incursion into the privacy and confidentiality of citizens. Any incursion into the requirement of such measures will be met with resistance by the Internet Industry.

- **Data Retention**

eco reminds the Commission on the ruling of the Court of Justice of the European Union (C-793/19, C-794/19) and the limits they imposed on data retention practices. eco underscores that any form of data retention is unacceptable as it infringes on the fundamental rights of EU citizens. With its member company Space.net, eco has successfully turned over data retention in the EU and is poised to do it again, should the European co-legislators again decide to infringe on the confidentiality of electronic communications.

- **Fighting cybercrime and terrorist content online**

The evaluation of the Terrorist Content Online Directive is currently in progress. Re-evaluation and revision of the existing regulatory framework should be based strictly on the empirical findings of this evaluation and include the experiences of digital platforms, Internet providers and civil society.

Identifying further measures to combat cybercrime beyond the already mentioned e-Evidence Framework is difficult and should be approached cautiously. eco welcomes the strengthening of competence within criminal authorities.

- **Boosting cooperation with tech platforms via the EU Internet Forum**

eco welcomes the fact that the Commission is also exploring collaborative approaches to counter misinformation. The Internet Industry acknowledges the developments that have unfolded in this field since the Forum' inception in 2015. Additionally, eco advises the Commission to focus strictly on illegal content and its countering. Disinformation poses a challenge and needs further research to better understand its impact on societies before any further legislative action can be explored. Currently, with the Digital Services Act in place, there should be no further regulation until its functioning is evaluated.

- **Digital technologies and artificial intelligence for improving law enforcement capabilities**

The use of digital technologies, especially Artificial Intelligence (AI) is strictly regulated in the EU. eco regards the provisions of the AI regulation on biometric real-time identification for law enforcement purposes as an asset in safeguarding human rights and strengthening trust in digital technology. The use of AI should be duly reviewed and strictly limited to measures that do not lead to profiling or wrongful presumptions that undermine the rule of law.

About eco: With approximately 1,000 member companies, eco (international.eco.de) is the leading Association of the Internet Industry in Europe. Since 1995, eco has been highly instrumental in shaping the Internet, fostering new technologies, forming framework conditions, and representing the interests of its members in politics and international forums. eco has offices based in Cologne, Berlin and Brussels. In its work, eco primarily advocates for a high-performance, reliable and trustworthy ecosystem of digital infrastructures and services.