Resolution No. 4

GA-2024-92-RES-04

Subject: The erosion of lawful access to digital evidence: impact on policing

The ICPO-INTERPOL General Assembly, meeting in Glasgow, United Kingdom, from 4 to 7 November 2024 at its 92nd session:

RECOGNIZING that effective policing requires lawfully authorized access to, and the competent examination of, relevant evidence by law enforcement authorities in order to prevent, investigate, and prosecute crime and to provide a path to justice for victims, and that a growing proportion of the aforementioned evidence is now manifest in digital form,

RECALLING INTERPOL's long-standing recognition of this issue, as evidenced in INTERPOL General Assembly Resolution GA-2021-89-RES-09 "Safeguarding children against online child sexual exploitation" (Istanbul, Türkiye, 23-25 November 2021), which expressed deep concern over the use by criminals of end-to-end encryption (E2EE) services to conceal their illicit online activities, while acknowledging the value of encryption to improve privacy, security, and the protection of fundamental rights,

MINDFUL of the increased interest in this issue in regional and international forums, such as the 2017 G20 Leaders' Statement on Countering Terrorism, which encouraged collaboration with industry to provide lawful and non-arbitrary access to available information where access is necessary for the protection of national security against terrorist threats; the 2023 G7 Interior and Security Ministers' Communiqué recalling the issue and committing to working to maintain tightly controlled lawful access to communications content that is vital to the investigation and prosecution of serious crimes; and the 2024 Joint Declaration of the European Police Chiefs on the matter of lawful access, which recognized the shared duty by law enforcement and the technology industry to keep the public safe,

ACKNOWLEDGING that the issue of technology companies providing for lawfully authorized access to digital evidence, while maintaining strong security and privacy are not mutually exclusive goals and that thoughtfully conceived and carefully implemented systems designed to enable lawful access to digital evidence, enhance both privacy and cybersecurity,

EXPRESSING PROFOUND CONCERN for the increasingly pervasive and unilateral rolling out of intractable E2EE communications and other technical services, which significantly challenge lawful access to digital evidence by law enforcement agencies, even when authorized to do so by competent judicial authorities within the relevant jurisdiction,

CALLS UPON all member counties, consistent with national legal frameworks, to exercise appropriate legislative and policy mechanisms, which will ensure technology companies implement technological solutions that enable law enforcement agencies to access critical digital evidence when legally authorized to do so;

ENCOURAGES member countries to regularly share information on how E2EE is being exploited by criminal actors with the aim of allowing INTERPOL to obtain an accurate global picture of the state of the threat and to provide member countries with such assessments;

ENCOURAGES member countries to share lawfully accessed data for the population of relevant INTERPOL Crime Analysis Files (CAFs) as appropriate and in line with the Organization's Constitution and Rules, including its Rules on the Processing of Data (RPD), in order to maintain INTERPOL's ability to provide operational and strategic threat assessments and investigative leads;

CALLS UPON the General Secretariat to provide guidance and best practices to member countries' law enforcement authorities within the framework of the Organization's capacity-building efforts, as well as assistance through INTERPOL global policing capabilities, to facilitate transnational lawful access requests by member countries' law enforcement authorities.

Adopted: 122 votes in favour, 1 against, 1 abstention