

# Recommendations for Tracing Networked Communications Across National Borders in Terrorist and Criminal Investigations

In October 1999, Justice and Interior Ministers of the G8 countries met in Moscow and directed their representatives to develop a concrete set of options for tracing networked communications across national borders in criminal investigations. The Ministers' Communiqué stated, in part:

**To ensure that we can all locate and identify criminals who use networked communications for illegal purposes, we must enhance our ability to trace communications while they are occurring and afterwards, even when those communications pass through multiple countries. Existing processes are often too slow and are designed more to address bilateral cooperation than crimes requiring the immediate assistance of many countries. Faster or novel solutions must be found.**

In May 2000, experts finalized a set of draft options. In July 2000, G8 Heads of State endorsed the undertaking of this work at their meeting in Okinawa, Japan. In February 2001, G8 Justice and Interior Ministers meeting in Milan called upon experts to develop specific traceability recommendations, taking into account relevant factors, specifically the protection of privacy and individual freedoms.

Ministers in Moscow also instructed experts to consult with industry representatives to seek their input related to traceability and other high-tech crime issues. Subsequently, conferences and workshops were held in Paris, Berlin and Tokyo, at which over one hundred representatives from high-tech companies around the world participated.

The tragic events of September 11, 2001 bring even greater urgency to this work. Terrorists can use E-mail, sites on the Internet, mobile phones, and other developing communication methods to make plans and transfer information across several continents in ways that make it difficult or impossible to trace those communications. Terrorists must not benefit from the modernization and globalization of communications. Therefore, we must work collectively to meet this challenge and enhance the abilities of all our Governments to combat terrorism and other criminal conduct.

Parallel challenges are presented by international high-tech crime cases, which can be committed at great distance. To succeed, investigators must trace a trail of communications to the source and victim computers or other devices, working with intermediate service providers in different countries. To locate the source of the crime, law enforcement often must rely on historical records that show when different connections were made, from where they were made, and who may have made them. At other times, law enforcement may also need to trace the connection as it is underway. When the providers fall outside the investigator's territorial jurisdiction, which they often do, law enforcement will usually need

help from counterparts in other jurisdictions. Traditional and even expedited mutual legal assistance measures are generally designed to obtain historical and real-time data in cases involving only two countries (e.g., the victim's country and offender's country). When a criminal routes communications through three, four, or five countries, the legal assistance process takes up successive periods before law enforcement can obtain data from each service provider farther up the trail of communications, increasing the chances the data will be unavailable or lost, and the criminal will remain unidentified and free to commit future criminal acts.

The Recommendations below propose a number of steps that Governments can take to allow them to trace more effectively international terrorist and criminal communications. The Recommendations address a broad range of issues, including preservation of data relating to specific investigations, expedited legal assistance, real-time tracing through multiple providers, and user-level authentication. The Recommendations are not intended to require providers to enhance existing technical capabilities. Finally, any implementation of these Recommendations is subject to domestic law and international obligations, with due regard for the adequate protection of human rights. To the extent possible, the Recommendations should be implemented in such a manner as to avoid or minimize the potential for conflicts among countries' laws, which can be an obstacle for both international law enforcement cooperation and cooperation between Governments and industry.

Governments should consider the following measures, which enhance the ability of law enforcement agencies to prevent and investigate terrorism and other criminal acts:

Allow service providers to retain identified categories of traffic data and/or subscriber data for legitimate business or public safety purposes, perhaps by supporting the adoption of best practice codes by service providers and service provider associations.<sup>(1)</sup>

1. Ensure data protection legislation, as implemented, takes into account public safety and other social values, in particular by allowing retention and preservation of data important for network security requirements or law enforcement investigations or prosecutions, and particularly with respect to the Internet and other emerging technologies.
2. Permit domestic law enforcement to serve foreign preservation instructions to domestic service providers after expedited approval, with substantive review if required by domestic law, through a domestic judicial or similar order.
3. Ensure the expeditious preservation of existing traffic data regarding a specific communication whether one or more service providers were involved in its transmission, and the expeditious disclosure of a sufficient amount of traffic data to enable identification of the service providers and path through which the communication was transmitted, through the execution of a single domestic judicial or similar order where permitted by domestic law.

Authorize domestic law enforcement to use the mechanisms described in the prior paragraph to respond to a foreign request, through expedited mutual assistance, even if there is no violation of the

domestic law of the requested State.<sup>(2)</sup>

4. Upon receiving a request from another State to trace a specific communication, authorize competent authorities, even if there is no violation of the domestic law of the requested State, to use mechanisms available under domestic law expeditiously to preserve all existing domestic data necessary to trace the communication, notify the requesting State if the communication appears to come from a third State, and provide sufficient data to the requesting State so that it may request assistance from the third State.
5. Authorize domestic law enforcement to trace in real-time specified communications in order to determine their path, origin or destination, including through multiple providers in a country, using a single domestic judicial or similar order if permitted under domestic law.
6. Authorize domestic law enforcement to use the mechanisms described in the prior paragraph to respond to a foreign request, through expedited mutual assistance, even if there is no violation of the domestic law of the requested State.
7. Encourage network architecture that improves security and allows, in appropriate cases, tracing of network abuses with due regard for the privacy of network users.
8. Encourage strong user-level authentication for appropriate applications, with due regard for technological neutrality and users' freedom of choice.

<sup>1</sup> The category or categories of data would be determined by each State. <sup>2</sup> The phrase "even if there is no violation of the domestic law of the requested State" is intended to signify that the requested State should provide assistance even if the conduct at issue does not meet all the conditions to qualify as a crime or cannot otherwise be prosecuted as a crime in that State. The phrase, and these Recommendations generally, are not intended to limit the possible imposition of other requirements for providing assistance that may be imposed by a requested State, including dual criminality requirements or exceptions for the essential interests of the requested State.