Data Preservation Checklists

At the G8 meeting of Justice and Interior Ministers in Moscow in October 1999, the Ministers recognized that law enforcement authorities conducting criminal investigations should, in some circumstances, be able to pursue investigations across territorial borders. As a first step, the Moscow Communiqué included *Principles on Transborder Access to Stored Computer Data* that detailed practical means to enable law enforcement expeditious access to data stored in other countries if that data was publicly accessible or was obtained with consent.

In addition, the Communiqué directed G8 experts "to develop, in consultation with industry, a concrete set of options for tracing networked communications across national borders in criminal investigations" and "to convene a conference where the G8 and industry can share ideas on Internet crime, with particular emphasis on issues relating to locating and identifying Internet criminals." To date, the G8 has hosted three *Government-Industry Dialogues on Safety and Confidence in Cyberspace:* Paris (May 15-17, 2000), Berlin (October 23-25, 2000), and Tokyo (May 22-24, 2001). These Dialogues provided an opportunity to discuss common problems and explore solutions associated with high-tech crime and the exploitation of the Internet for criminal purposes. The primary issues addressed in the Dialogues were: data retention, data preservation, real-time tracing, threat assessment and prevention, and training.

During the course of these consultations, the High-Tech Crime Subgroup developed *"Recommendations for Tracing Networked Communications Across National Borders in Terrorist and Criminal Investigations,"* which contain specific elements regarding data preservation when multiple jurisdictions are involved.

Data preservation does not compel either collection or retention of data; it is essentially a "do-not-delete" order pertaining to existing data. A data preservation scheme provides that upon a lawfully authorized request, based on the facts of a specific case, particular data that has already been collected can be preserved to prevent its deletion. At a later point, a lawful request by a competent authority can compel disclosure of the data.

Thirty-three countries have signed the Council of Europe *Convention on Cybercrime*. The *Convention* contains provisions for data preservation, and a number of countries are currently analyzing the necessity of new legislation or exploring legislative options to implement a data preservation scheme in their countries.

In order to assist countries in this task, the High-Tech Crime Subgroup has developed the following practical tools: a list of issues that could be considered in any current or possible future legal framework for data preservation and a checklist of best practices for law enforcement requests for preservation of data. These tools were products of the G8 Government-Industry dialogue in Tokyo. Although the G8 Subgroup on High-Tech Crime does not intend these documents to be binding on countries, the documents provide guidance and assistance to countries considering data preservation legislation and to law enforcement agencies in carrying out data preservation requests.

Issues to Be Considered in a Legal Framework for Data Preservation

Purpose: The purpose of this document is to set forth a series of questions that could be considered in any current or possible future legal framework for data preservation.

Note: For purposes of this document, the term "Preservation" shall mean that (a) upon lawful request by a competent authority, (b) based on the facts of a specific case, (c) specific *historical* data can be preserved to prevent its deletion, (d) pending issuance of a lawful demand from a competent authority to disclose the data. "Preservation" does not include prospective collection of data and does not obligate a service provider to generate data not already in existence.

1. Source of Law

    1.1 What is the basis in procedural law for a Preservation Order?

    1.2 Are there substantive legal predicates for issuance of a Preservation Order?

1.3 Are there substantive legal predicates for a Preservation Order to cover specific types of data (e.g. traffic data vs. content)?

2. Scope

What records should be subject to a Preservation Order?

3. Duration of Preservation Order

For how long should the records by preserved?

4. Form of Preservation Order

4.1 Should there be a standardized form for Preservation Orders?

4.2 Should the form of delivery for Preservation Orders be:

- Written only
- Verbal
- Verbal, followed by written confirmation
- E-mail

5. Authorized Issuers

5.1 What competent authorities ("Issuers") can issue a Preservation Order?

5.2 Should there be authentication measures to identify communications initiated by an Issuer?

6. Geographic Scope

Can a Preservation Order apply to:

6.1 Records located outside jurisdiction of Issuer?

6.2 Recipients located outside jurisdiction of Issuer?

7. Confidentiality

7.1 Can the Issuer require that the Recipient (a) maintain the confidentiality of the Preservation Order and/or (b) keep the Preservation Order confidential from the subject of the investigation?

7.2 What is the penalty for such unauthorized disclosure?

7.3 Should there be a deadline or expiration point for any confidentiality requirement?

8. Reimbursement of Recipient

Is reimbursement available to a Recipient? What costs can be recovered by the Recipient?

9. Class of Recipients

9.1 What entities ("Recipients") can be served with a Preservation Order?

9.2 What individuals or departments within a Recipient entity should receive the Preservation Order?

9.3 Can a single Preservation Order apply to multiple Recipients within a single jurisdiction? Can it apply to multiple Recipients in different jurisdictions within the same country?

10. Immunity of Recipient

Is immunity from legal action available to a Recipient in connection with its compliance with a lawful Preservation Order? Specifically, is this immunity:

10.1 Criminal immunity?

10.2 Civil immunity?

10.3 Foreign immunity?

11. Penalty for Non-Compliance

What penalty (if any) would be imposed on a Recipient who does not undertake an authorized Preservation Order?

12. Recipient's Right of Refusal

Under what circumstances is a Recipient justified in seeking clarification, modification, or otherwise not complying with a Preservation Order?

13. Duty to Revoke

Does the Issuer have a duty to revoke the Preservation Order when the Issuer no longer believes that a related disclosure order will follow?

14. Scope of Use

Can preserved data be disclosed and used pursuant to other legal process (e.g. civil subpoena) or is disclosure and use limited to the specific criminal investigation forming the basis for the Preservation Order?

15. Interaction with Mutual Legal Assistance Obligations

15.1 Is the Preservation Order process consistent with the MLA process?

15.2 What criteria (if any) should be considered when deciding whether to issue a Preservation Order at the request of a foreign competent authority?

15.3 Is a Preservation Order appropriate or possible when preservation is sought by a foreign competent authority and the recipient competent authority considers that there may be no apparent dual criminality for the underlying incident under investigation?

16. Partial Disclosure

Should some form of partial disclosure be authorized or required in order to identify other potential Recipients who may possess data relevant to the investigation?

17. Potential Abuses

What practices or outcomes would be considered an abuse of the preservation process?

18. Potential Conflicting Laws

What laws may conflict with the requirements of a Preservation Order?

19. Disclosure Standards

What standards govern disclosure of data preserved pursuant to a lawful Preservation Order?

20. Dispute Resolution

What authority (court, commission, etc.) can resolve disputes relating to the validity or scope of a Preservation Order?

Law Enforcement Record

Preservation Checklist

Purpose: This checklist is intended to be used by individuals working for a competent authority, when issuance of a Preservation Order is possible, in the context of a specific criminal investigation.

Note: For purposes of this checklist, the term “Preservation” shall mean that (a) upon lawful request by a competent authority, (b) based on the facts of a specific case, (c) specific historical data can be preserved to prevent its deletion, (d) pending issuance of a lawful demand from a competent authority to disclose the data. “Preservation” does not include prospective collection of data and does not obligate a service provider to generate data not already in existence.

1. Identify Source of Preservation Request

1.1 Domestic

1.2 Foreign

2. Identify Legal Basis for Preservation Order

2.1 Law authorizing issuance of the Preservation Order

2.2 Underlying criminal offence forming basis for the Preservation Order

3. Identify Appropriateness and Extent of Preservation Order

3.1 Is the issuance of the Preservation Order, and the extent of the Order, appropriate? For example, are the Preservation Order and the records requested to be preserved (a) proportional; (b) relevant to the investigation; or (c) not unreasonably burdensome on the Recipient?

3.2 Are the records publicly available?

4. Identify What Information Law Enforcement Already Possesses

4.1 Individual’s identity (e.g. name)

4.2 Account name (e.g. joe@internetmail.com)

4.3 Communication (e.g. E-mail from A to B)

4.4 File (e.g. graphic, text etc.)

5. Identify Recipient(s) of Preservation Order

5.1 What entity ("Recipient") should receive the Preservation Order?

5.2 What department or individual within the Recipient entity should receive a copy of the Preservation Order?

6. Identify Records to be Preserved

The following types of records may be available from a typical Internet service. It should be noted that not all of the following types of data elements will be available from every Recipient, and that actual records available will depend upon the Recipient's business model and record retention practices.

6.1 Subscriber Records (e.g. subscriber name, physical address)

6.2 Traffic Data (e.g. Userid, assigned IP address) Note: The Council of Europe Cybercrime Convention contains a definition of Traffic Data.

6.3 Stored Content (e.g. stored E-mail, stored FTP files)

6.4 Other Relevant Information

7. Define Scope of Preservation Order

7.1 Time Period for Preservation by Recipient

7.2 Time Span for Relevant Records

8. Reimbursement for Recipient

Are there any laws, policies, or arrangements for the reimbursement of costs?

9. Identify Proper Means for Service of Preservation Order on Recipient

9.1 Written

9.2 Verbal

9.3 Verbal, followed by written confirmation

9.4 E-mail

10. Prepare Follow-up Plan to Obtain Disclosure