erpastudies

europol

ELECTRONIC RESOURCE PRESERVATION AND ACCESS NETWORK

erpanet

www.erpanet.org

ERPANET – Electronic Resource Preservation and Access Network – is an activity funded by the European Commission under its IST programme (IST-2001-3.1.2). The Swiss Federal Government provides additional funding.

Further information on ERPANET and access to its other products is available at http://www.erpanet.org.

A great deal of additional information on the European Union is available on the Internet. It can be accessed through the Europa server (http://europa.eu.int).

ISSN 1741-8682

ELECTRONIC RESOURCE PRESERVATION AND ACCESS NETWORK

Table of Contents

Executive Summary

Europol is the European Union organisation that handles criminal intelligence and analysis of criminal activities across Europe. Established in the 1990s, Europol acts on request to support the law enforcement activities of the Member States in situations where an organised criminal structure is involved and two or more Member States are affected. Europol's mandate includes all forms of serious crime as mentioned in the Annex of the Europol Convention, including illicit trafficking of drugs, human-beings and vehicles, and money laundering, cyber-crime, and terrorism.

As a cross-border criminal intelligence and analysis agency, Europol receives information in a wide array of formats from countries across the European Union. The Europol Convention clearly states their responsibilities with regards to this information and the data they may keep on human subjects. As a result, Europol have surprisingly few concerns with regards to the long-term preservation of operational data. Although they use electronic records on a daily basis, legal responsibility for maintaining much of it lies elsewhere. Their concerns rest primarily with maintaining secure and reliable data during the time they are awarded it, and with timely destruction of the data at the end of that period. However, short to medium term preservation is required for their organisational digital records. To achieve this, Europol is staggering implementation of an electronic record keeping system throughout the organisation. They intend to tackle preservation issues when implementation is complete, although this may result in some problems later as preservation is always best considered from the outset.

In the context of the ERPANET suite of case studies and their focus on digital preservation, Europol cannot be taken as representative of other European organisations engaged in crime-fighting activities. It is included here in order to highlight the different circumstances in which digital information is used and exchanged, and the importance of clearly delineated legal responsibility for information preservation and destruction.

Chapter 1: The ERPANET Project

The European Commission and Swiss Confederation funded ERPANET Project[1] (Electronic Resource Preservation and Access Network) works to enhance the preservation of cultural and scientific digital objects through raising awareness, providing access to experience, sharing policies and strategies, and improving practices. To achieve these goals ERPANET is building an active community of members and actors, bringing together memory organisations (museums, libraries and archives), ICT and software industry, research institutions, government organisations, entertainment and creative industries, and commercial sectors. ERPANET constructs authoritative information resources on state-of-the-art developments in digital preservation, promotes training, and provides advice and tools.

ERPANET consists of four partners and is directed by a management committee, namely Seamus Ross (HATII, University of Glasgow; principal director), Niklaus Bütikofer (Schweizerisches Bundesarchiv), Hans Hofman (Nationaal Archief/National Archives of the Netherlands), and Maria Guercio (ISTBAL, University of Urbino). At each of these nodes a content editor supports their work, and Peter McKinney serves as a co-coordinator to the project. An Advisory Committee with experts from various organisations, institutions, and companies from all over Europe give advice and support to ERPANET.

[1] ERPANET is a European Commission funded project (IST-2001-32706). See www.erpanet.org for more details and available products.

Chapter 2: Scope of the Case Studies

While theoretical discussions on best practice call for urgent action to ensure the survival of digital information, it is organisations and institutions that are leading the drive to establish effective digital preservation strategies. In order to understand the processes these organisations are undertaking, ERPANET is conducting a series of case studies in the area of digital preservation. In total, sixty case studies, each of varying size, will investigate awareness, strategies, and technologies used in an array of organisations. The resulting corpus should make a substantial contribution to our knowledge of practice in digital preservation, and form the foundation for theory building and the development of methodological tools. The value of these case studies will come not only from the breadth of companies and institutions included, but also through the depth at which they will explore the issues.

ERPANET is deliberately and systematically approaching disparate companies and institutions from industry and business to facilitate discussion in areas that have traditionally been unconnected. With these case studies ERPANET will broaden the scope and understanding of digital preservation through research and discussion. The case studies will be published to improve the approaches and solutions being developed and to reduce the redundancy of effort. The interviews are identifying current practice not only in-depth within specific sectors, but also cross-sectorally: what can the publishing sector learn from the aeronautical sector? Eventually we aim to use this comparative data to produce intra-sectoral overviews.

This cross-sectoral fertilisation is a main focus of ERPANET as laid out in its Digital Preservation Charter.[2] It is of primary importance that disparate groups are given a mechanism through which to come together as best practices for digital preservation are established in each sector.

Aims

The principal aims of the study are to:

- build a picture of methods and match against context to produce best practices;
- accumulate and make accessible information about practices;
- identify issues for further research;
- enable cross-sectoral practice comparisons;
- enable the development of assessment tools;
- create material for training seminars and workshops; and,
- develop contacts.

Potential sectors have been selected to represent a wide scope of information production and digital preservation activity. Each sector may present a unique perspective on digital preservation. Organisational and sectoral requirements, awareness of digital preservation, resources available, and the nature of the digital

[2] The Charter is ERPANET's statement on the principles of digital preservation. It has been drafted in order to achieve a concerted and co-ordinated effort in the area of digital preservation by all organisations and individuals that have an interest and share these concerns. http://www.erpanet.org/charter.php.

object created place unique and specific demands on organisations. Each of the case studies is being balanced to ensure a range of institutional types, sizes, and locations.

The main areas of investigation included:

- perception and awareness of risk associated with information loss;
- understanding how digital preservation affects the organisation;
- identifying what actions have been taken to prevent data loss;
- the process of monitoring actions; and,
- mechanisms for determining future requirements.

Within each section, the questions were designed to bring organisational perceptions and practices into focus. Questions were aimed at understanding impressions held on digital preservation and the impact that it has had on the respective organisation, exploring the awareness in the sector of the issues and the importance that it was accorded, and how it affected organisational thinking. The participants were asked to describe, what in their views, were the main problems associated with digital preservation and what value information actually had in the sector. Through this the reasons for preserving information as well as the risks associated with not preserving it became clear.

The core of the questionnaire focused on the actions taken at corporate level and sectoral levels in order to uncover policies, strategies, and standards currently employed to tackle digital preservation concerns, including selection, preservation techniques, storage, access, and costs. Questions allowed participants to explore the future commitment from their organisation and sector to digital preservation activities, and where possible to relate their existing or planned activities to those being conducted in other organisations with which they might be familiar.

Three people within each organisation are targeted for each study. In reality this proved to be problematic. Even when organisations are identified and interviews timetabled, targets often withdrew just before we began the interview process. Some withdrew after seeing the data collection instrument, due in part to the time/effort involved, and others (we suspect) dropped out because they realised that the expertise was not available within their organisation to answer the questions. The perception of risks that might arise through contributing to these studies worried some organisations, particularly those from sectors where competitive advantage is imperative, or liability and litigation issues especially worrying. Non-disclosure agreements that stipulated that we would neither name an organisation nor disclose any information that would enable readers to identify them were used to reduce risks associated with contributing to this study. In some cases the risk was still deemed too great and organisations withdrew.

Chapter 3: Method of Working

Initial desk-based sectoral analysis provides ERPANET researchers with essential background knowledge. They then conduct the primary research by interview. In developing the interview instrument, the project directors and editors reviewed other projects that had used interviews to accumulate evidence on issues related to digital preservation. Among these the methodologies used in the Pittsburgh Project and InterPARES I for target selection and data collection were given special attention. The Pittsburgh approach was considered too narrow a focus and provided insufficient breadth to enable full sectoral comparisons. On the other hand, the InterPARES I data collection methodology proved much too detailed and lengthy, which we felt might become an obstacle at the point of interpretation of the data. Moreover, it focused closely on recordkeeping systems within organisations.

The ERPANET interview instrument takes account of the strengths and weaknesses from both, developing a more focused questionnaire designed to be targeted at a range of strategic points in the organisations under examination. The instrument[3] was created to explore three main areas of enquiry within an organisation: awareness of digital preservation and the issues surrounding it; digital preservation strategies (both in planning and in practice); and future requirements within the organisation for this field. Within these three themes, distinct layers of questions elicit a detailed discovery of the state of the entire digital preservation process within participants' institutions. Drawing on the experience that the partners of ERPANET have in this method of research, another important detail has been introduced. Within organisations, three categories of employee were identified for interview: an Information Systems or Technology Manager, Business Manager, and Archivist / Records Manager. In practice, this usually involved two members of staff with knowledge of the organisation's digital preservation activities, and a high level manager who provided an overview of business and organisational issues. This methodology has allowed us to discover the extent of knowledge and practice in organisations, to understand the roles of responsibility and problem ownership, and to appreciate where the drive towards digital preservation is initiated within organisations.

The task of selecting the sectors for the case studies and of identifying the respective companies to be studied is incumbent upon the management board. They compiled a first list of sectors at the very beginning of the project. But sector and company selection is an ongoing process, and the list is regularly updated and complemented. The Directors are assisted in this task by an advisory committee.[4]

[3] See http://www.erpanet.org/studies/index.php. We have posted the questionnaire to encourage comment and in the hope that other groups conducting similar research can use the ideas contained within it to foster comparability between different studies.
[4] See www.erpanet.org for the composition of this committee.

Chapter 4: Europol

http://www.europol.eu.int/

Europol is the European Union law enforcement organisation that handles criminal intelligence and analysis of criminal activities across Europe. The establishment of Europol was formally agreed in the Maastricht treaty of 1992.[5] Limited operations were started in 1994 and, after ratification of the Europol Convention[6] by all Member States[7] in 1998, Europol commenced full activities on 1 July 1999. Based in The Hague, Europol employs approximately 400 staff from across all the Member States. It is divided into five departments which cover Serious Crime, Information and Communication Technology (ICT), Information Management (IM), Resources, and Corporate Governance & Development, each with several units. Financed by contributions from the Member States according to their GNP (Gross National Product), the organisation is democratically controlled and accountable to the Council of Ministers of the EU responsible for Justice and Home Affairs (JHA).[8]

The aim of Europol is to improve the effectiveness and cooperation between the competent authorities of the Member States in preventing and combating serious international organised crime. To this end, Europol supports and provides information exchange and analysis, but is not an executive body and has no executive powers. Europol does not itself carry out law enforcement, but supports the law enforcement activities of the Member States in cases where an organised criminal structure is involved and two or more Member States are affected. Europol's mandate includes all forms of serious organised crime as mentioned in the annex of the Europol Convention and activities are directed mainly against illicit trafficking of drugs, vehicles, and people (including child pornography), counterfeiting of the Euro and other forms of payment, money-laundering, and cyber crime.

Europol acts only on request by a competent authority[9] of a Member State, which contributes original data to substantiate the investigation and which provides the foundation for Europol's analysis. Operating within the framework of the Europol Convention,[10] Europol supports the activities of Member States by facilitating information exchange, providing operational analysis that supports Member States' operations, and generating strategic reports and crime analysis on the basis of information and intelligence supplied by Member States or generated by Europol. It

---

[5] Maastricht Treaty on European Union, 7 February 1992. See http://europa.eu.int/en/record/mt/top.html.

[6] Europol Convention, published in the Official Journal of the European Communities (OJEC), 27 November 1995, C316/2. The Europol Convention is also available at Europol's website, see: http://www.europol.eu.int/index.asp?page=legalconv.

[7] Following EU enlargement in May 2004, there are now twenty-five Member States in total and more applications pending.

[8] The Council of Ministers for the EU responsible for Justice and Home Affairs meets approximately once per month and is comprised of the Member States' Ministers for Justice and Home Affairs. See http://ue.eu.int/cms3_fo/showPage.asp?id=249&lang=EN for more information.

[9] 'Competent Authorities' are those authorities responsible under national law for preventing and combating criminal offences (as defined in the Council of the European Union Act of 12 March 1999, on adopting the rules governing the transmission of personal data by Europol to third states and third bodies. Published in the Official Journal of the European Communities 1999/C 88/01, available at: http://www.europol.eu.int/legal/other/files/OJEC_1999C88_01_TransmPersData_en.pdf.

[10] Europol Convention, op cit.

provides expertise and technical support for investigations and operations carried out within the EU, under the supervision and legal responsibility of the Member States concerned.

The Europol Convention stipulates Europol's responsibilities with regards to the collection, processing, and utilization of personal data, which conform to the Council of Europe Convention of 1981 regarding the Automatic Processing of Personal Data (exceptions noted). [11] Due to regards for the privacy of the individual and the ultimate responsibility of the Member States, Europol's emphasis in records management lies not so much on preservation, but on effective life-cycle management of the records whilst in Europol's care, and their required timely destruction. Europol embarked on preparations for a staggered electronic document and records management system implementation for their internal digital records in late 2002. The document management system has now been installed and will be expanded to include a full records management environment by late 2005. In the current absence of full digital records management, Europol maintains a small paper archive for administrative documentation that is managed by the Directorate Support unit. Operational, financial, and personnel files are kept in decentralised paper archives.

For reasons of operational security, this study does not include detailed information on, nor analysis of, Europol's operational systems. The focus is on Europol's internal organisational records. Operational records are discussed only when such information is freely available or does not pose a security risk.

[11] For further information on this Convention, see the Council of Europe website: http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=108&CM=8&CL=ENG.

Chapter 5: Details and circumstances of the interviews

ERPANET first approached Europol with a view to case study participation in October 2003. Europol were then in the process of installing a Document Management System (DMS) so interviews were delayed until rollout was complete. Interviews took place at the Europol premises in The Hague during April and May 2004 and were separately attended by the DMS project manager Mr Armin Reif, Assistant Director and Head of IT Mr Casper van den Wall Bake, and Assistant Director and Head of Resources Mr Leo van Kampen.

A further interview took place in June to discuss aspects of records management. This was attended by Mr Reif and also Mr Axel Szablikowski of the Directorate Support Unit, responsible for maintaining the centralised paper archive. Additional information was supplied by email.

Chapter 6: Analysis

This section presents an analysis of the data collected during the case study. It is organised to mirror the sequence of topics in the questionnaire.

- Perception and Awareness of Digital Preservation
- Preservation Activity
- Compliance Monitoring
- Digital Preservation Costs
- Future Outlook

Perception and Awareness of Digital Preservation

Digital Preservation is considered an important issue at Europol, but not from the usual long-term sense. Instead, digital preservation is viewed from the perspective of the integrity and reliability of digital information maintained in their systems – preserving the reliability and integrity of digital information in their care, as opposed to concerted efforts to preserve it over and through time. The relatively young age of the organisation may be a factor in this, but, as will become apparent below, this is primarily due to their operational and legislative context.

The main problems

Staff working directly with IT systems were aware of the general problems caused by wide-ranging hardware and software obsolescence and the challenges this posed for digital preservation over the long term. Due to the legislative context identified below, they do not consider this a significant problem for them. More important is maintaining the reliability and integrity of the information whilst in their safekeeping. Staff showed appreciation of the records life-cycle, with particular emphasis on records destruction as Europol's legislative context demands that much of its data is completely destroyed after only a very short period of time. This alone can be a significant challenge in a digital environment that allows multiple copies of records to exist across a large and multi-lingual network.

This level of knowledge was not reflected in staff working outside of IT or the DMS Project, and respondents reported little knowledge of sectoral or other collaborative efforts to tackle digital preservation problems.

Asset value and risk exposure

Europol create and receive different types of records in a wide range of digital formats. There are two general types of data: operational data regarding investigations; and, organisational, administrative data. Most operational data is contributed by Member States for analysis by Europol, although Europol itself also generates operational data through its analysis and the results of its investigations. Organisational data is generated on a day-to-day basis, including administrative and financial data. Staff were aware of the high usability value of all of these types of information in digital form, thus the emphasis on information integrity and maintaining high quality data shown by those in IT and the DMS project.

Europol's retention responsibilities are limited by their status as a non-executive body, and as its operational data has a very limited retention period, it considers such data to be at little or no risk from serious digital preservation issues. That said, staff

appreciated that the organisation's professional reputation would be damaged should they lose data, and that questions would be asked in the Commission. Regarding their organisational data, which is maintained in the newly installed DMS (Hummingbird), they are aware of their responsibilities and cited possible legal and financial consequences for failing to meet them. However, their greatest concern lies in ensuring the reliability and security of operational data whilst in their care.

Regulatory Environment

The Europol Convention of 1995 is Europol's primary legislative framework. This convention covers the establishment of Europol and its tasks, and details the organisations legal status, organisational and financial provisions, as well as liability and legal protection. It also defines many aspects of their information system, and specifies common provisions that must apply between Europol and the Member States on information processing.

Several Articles of the Convention concern the maintenance and preservation of Europol's operational information assets that are submitted by the Member States. Article 3 of the Convention states that one of Europol's tasks shall be 'to maintain a computerised system of collected information containing data in accordance with Articles 8, 9, and 10'.[12] These articles relate to content, rights of access, and the collection, processing and utilisation of personal data in Europol's information system. Furthermore, Article 21 of the convention stipulates time limits for the storage and deletion of data files and limits Europol's retention of operational data to 'only as long as is necessary for the performance of its tasks'. The need for continued storage must be reviewed no later than three years after the input of data, and if no longer required, the data must be destroyed. The need for continued storage is judged by the participants in the analysis, in accordance with Article 10(8) of the Europol Convention. Where no agreement can be reached, a decision is taken by the Management Board.[13] A very strong case must be made for information to be kept, and the data subject must agree to the continued storage – in practice, this results in the destruction of operational data after three years in the vast majority of cases. There are provisions for extenuating circumstances, but the emphasis is on data destruction, not on preservation. Ownership and legal responsibility of submitted information remains with the Member State that contributed it, and not with Europol.

There is no specific Europol legislation with regard to administrative information, so, as with other European and International agencies,[14] the organisation must recourse to the legislation of the country in which they are residing as regards their administrative records, in this case the Netherlands.

Preservation Activity

Due to the very short operational data retention periods stipulated in their Convention, preservation activity at Europol is negligible. Their current focus is on implementing electronic document management for their administrative records and reports, for example, annual reports, or reports generated by Europol as a result of an

[12] See Europol Convention, op. cit.
[13] As stated in the Council Act of 3 November 1988 on Adopting Rules Applicable to Europol Analysis Files (1999/C 26/01). See: http://www.europol.eu.int/index.asp?page=AWfiles_regs_en.
[14] See for example the ERPANET case study on the World Intellectual Property Organisation (WIPO), http://www.erpanet.org/studies/.

investigation. Electronic records management will follow, the final stages of which are scheduled for 2005.

As a result of the Convention, there are no measures in place for the long-term preservation of Europol's digital operational data. The following sections will therefore focus largely on Europol's implementation of an electronic document/records management system for its administrative records and strategic reports for management.

Policies and Strategies

Preservation of digital resources has not yet been explicitly incorporated into Europol's document management project, although the DMS project manager intends to incorporate in the final stages of electronic records management implementation. There are therefore no written policies or strategies in place for preserving information in digital form. Europol's focus on operational activities and their emphasis on adhering to professional standards of information integrity and data destruction means that long term preservation simply has not yet become a great issue for them.

Selection

Europol's approach to records management hinges around staggered implementation of their electronic record keeping system, which is currently still at a document management stage. When the system has been fully implemented, all official documents must be entered and managed through it; up until this time, staff are free to choose which documents they enter. This 'anything goes' strategy was chosen specifically so that staff had the opportunity to get used to working with the DMS, as technologies are often viewed with suspicion by users when they are first implemented.

The DMS has a built-in classification schedule that incorporates confidentiality levels, ranging from public to confidential. These levels are identified in the Council Act of 3 November 1998 on adopting rules on the confidentiality of Europol information.[15] The DMS will in future link to a retention schedule covering all selected documents.

Responsibility for maintenance of these schedules lies with the Data Protection Officer.

Preservation

Documents in the DMS are 'preserved' at a very basic level. They are kept in their original format, often proprietary, with the final format depending on the individual preferences of the person in charge. Europol developed their own metadata profile for each document, consisting of twenty-five elements. Only six of these are mandatory. The majority of fields are completed via drop-down options, minimising the risks of human error, and the system automatically determines file formats.

The IT department takes regular backups of the system, but is focused more on security and disaster recovery than long-term maintenance of the data.

Access

Only authorised Europol personnel can access the system and contents. The user interface is available only in English, although the contents may be in any of the official

[15] Published in the *Official Journal of the European Communities,* 30.1.1999.

languages of the EU. Security and auditing measures in place but cannot be discussed here.

Compliance Monitoring

There are no specific auditing measures regarding preservation of data planned outside of Europol's regular auditing procedures

Digital Preservation Costs

Europol carry out cost investment analysis for all investments but participants were unable to provide specific details. They believe that future costs for maintaining and preserving data will, in the absence of a specified and dedicated group, come from the IT budget.

Future Outlook

Respondents were aware that their current approach is not sufficient to properly preserve information for the long term. Given the relatively short retention periods for most of their data, they are not unduly concerned about this. They expect accessibility to their records, whichever format they may be in, for as long as they are required, although they are aware that files in old and proprietary formats will prove difficult to access with the passage of time. They intend to expand their approach by moving to a records management system, and staff on the DMS project will consider the need for preservation explicitly during that period.

Chapter 7: Conclusions

Europol are in a fortunate position whereby long-term digital preservation does not appear to pose significant problems for them. The young age of the organisation and its legislative environment are primary factors in this. As a non-executive body, Europol produces few (if any) records requiring long-term retention. Much of the data used during the course of investigations originates from and belongs to Member States, absolving Europol of the need to preserve it. Few other organisations are likely to find themselves in such a position.

Despite this, Europol may yet experience some problems maintaining their digital administrative and organisational records over the short to medium term. This is due to the insufficient regard so far paid to the general aspects of their approach that affect records kept for any amount of time – files are kept in proprietary formats with insufficient record keeping metadata and authenticity cannot be guaranteed. Furthermore, it is unlikely that they will be able to rely on their current digital records should legislation change and the retention periods are extended.

Preservation is most successful if it is considered from the outset. ERPANET's experience shows that organisations attempting to tack digital preservation onto the end of their records management solution invariably find it to be less efficient than if it had been considered from the outset: for example, the manner in which records are created has an often underestimated effect on the records' chances for long term, authentic survival; if they are not created in an appropriate and stable manner to begin with, they will not last for long in an ever-changing technical environment. In addition, costs may well be significantly higher, increased by new requirements for conversion of files into new formats more appropriate for record storage and additional metadata requirements that involve manual data entry (probably by different personnel to the record creators, which brings further levels of risk). Whilst Europol, given the scale of the records collection and their current restrictive legislative framework, may not suffer greatly in this respect, these are certainly issues which organisations should consider as soon as possible in the records life-cycle and their active management of it.

Appendix 1: References

All information pertaining to this study can be located through the following sites:

ERPANET website: http://ww.erpanet.org/.

Europol website: http://www.europol.eu.int/.

Europa website – Gateway to the European Union: http://europa.eu.int/.

erpanet

CONTACT DETAILS

ERPANET Coordinator
George Service House
11 University Gardens,
University of Glasgow
Glasgow, G12 8QQ,
Scotland

Tel: +44 141 330 4568
Fax: +44 141 330 3788
Coordinator@erpanet.org

ERPANET STAFF

www.erpanet.org