European Cooperation
in the field of Scientific
and Technical Research
- COST -

Brussels, 21 November 2012

IC1206

MEMORANDUM OF UNDERSTANDING

Subject : Memorandum of Understanding for the implementation of a European Concerted Research Action designated as COST Action IC1206: De-identification for privacy protection in multimedia content

Delegations will find attached the Memorandum of Understanding for COST Action as approved by the COST Committee of Senior Officials (CSO) at its 186th meeting on 20 - 21 November 2012.

MEMORANDUM OF UNDERSTANDING
For the implementation of a European Concerted Research Action designated as

COST Action IC1206
DE-IDENTIFICATION FOR PRIVACY PROTECTION IN MULTIMEDIA CONTENT

The Parties to this Memorandum of Understanding, declaring their common intention to participate in the concerted Action referred to above and described in the technical Annex to the Memorandum, have reached the following understanding:

1. The Action will be carried out in accordance with the provisions of document COST 4154/11 “Rules and Procedures for Implementing COST Actions”, or in any new document amending or replacing it, the contents of which the Parties are fully aware of.

2. The main objective of the Action is to establish mechanisms for sharing knowledge and technology in different (scientific, legal, ethical and societal) fields related to automated de-identification and reversible de-identification for privacy protection in multimedia contents.

3. The economic dimension of the activities carried out under the Action has been estimated, on the basis of information available during the planning of the Action, at EUR 56 million in 2012 prices.

4. The Memorandum of Understanding will take effect on being accepted by at least five Parties.

5. The Memorandum of Understanding will remain in force for a period of 4 years, calculated from the date of the first meeting of the Management Committee, unless the duration of the Action is modified according to the provisions of Chapter V of the document referred to in Point 1 above.

A. ABSTRACT AND KEYWORDS

De-identification in multimedia content can be defined as the process of concealing the identities of individuals captured in a given set of data (images, video, audio, text), for the purpose of protecting their privacy. This will provide an effective means for supporting the EU's Data Protection Directive (95/46/EC), which is concerned with the introduction of appropriate measures for the protection of personal data. The fact that a person can be identified by such features as face, voice, silhouette and gait, indicates the de-identification process as an interdisciplinary challenge, involving such scientific areas as image processing, speech analysis, video tracking and biometrics. This Action aims to facilitate coordinated interdisciplinary efforts (related to scientific, legal, ethical and societal aspects) in the introduction of person de-identification and reversible de-identification in multimedia content by networking relevant European experts and organisations.

Keywords: De-Identification, Reversible De-Identification, Biometrics, Privacy Protection, Multimedia

B. BACKGROUND

B.1 General background

Recent advances in audio recording devices, cameras, web technology and signal processing have highly facilitated the efficacy of audio and video acquisition. This capability is now widely exploited in a variety of scenarios to capture audio-video recordings of people, either for immediate inspection or for storage and subsequent analysis and sharing. Moreover, the widespread use of video surveillance cameras and intelligent networks of sensors in public locations (streets, squares, train stations, subway stations, airports, stores, schools, automated teller machines (ATMs)), and the use of reliable biometric-based recognition software enable identification and tracking of people in real time.

Whilst it is recognised that there are justified reasons for sharing multimedia data acquired in such manners (e.g. low enforcement, forensics, bioterrorism surveillance), there is also a strong need for protecting the privacy of the guiltless individuals who are inevitably captured in the recordings. Indeed, such privacy concerns are further ignited by the continued increase in the deployment of audio/video recording technologies. The technologies like "Google Street View" and

“EveryScape” provide an additional framework for the invasion of the individuals’ privacy, as people present on the scene are not aware of the video acquisition and their consent for it is not taken.

In general, privacy can be defined as the ability of an individual or group to have their personal information and affairs secluded from others, and to disclose them as they choose. Privacy concerns exist wherever personal data or personal (identifiable) information is collected and stored – in digital form or otherwise. Personal data mean any information relating to an identifiable person ("data subject"). An identifiable person is one who can be identified, directly or indirectly, in particular with reference to an identification number or to one or more factors specific to his physical, physiological, habitual, mental, economic, cultural or social identity.

The 1995 Data Protection Directive of the European Union (Directive 95/46/EC) is an operating basic model for handling personal data. It demands the deployment of appropriate technical and organisational measures to protect private information in the course of transferring or processing such data. This legal requirement along with ethical responsibilities has restricted data sharing and utilisation while various organisations may require the use of such data for research, business, academic, security and many other purposes. The directive defines the following six basic principles of the Fair Information Practices: (i) existence of personal data collections should be public knowledge, (ii) individuals have a right to review and correct their information, (iii) the minimum information necessary should be collected, and where appropriate, consent of the included individuals should be obtained, (iv) personal data should be accurate and complete and retained only for the given time period, (v) data should be only used for the purpose originally intended, (vi) data should be protected by security safeguards against unauthorized access, modification or use.

In July 2008, the Information Commissioner’s Office (ICO) commissioned a review of the 1995 EU Data Protection Directive (95/46/EC). In 13 years since the Directive came into force, the world has seen dramatic changes in the way personal data is accessed, processed and used. At the same time, the general public has become increasingly aware of the potential danger for their personal data to be abused. Based on analysing strengths and weaknesses associated with the Directive, and with reference to the continued technological changes and the move towards a globally networked society, the ICO has identified a set of distinct challenges, such as: (i) defining privacy – when privacy is affected by personal data processing and when it is not, how strong the link between data protection regulations and privacy protection should be; (ii) risk assessment – can it be predicted how risky it is to provide our personal data to an entity or organisation? (iii) rights of the individual in relation to the benefit of society – under what circumstances can personal privacy become secondary to the needs of society, considering the fundamental importance of privacy protection for the development of a democratic society as a whole? (iv) transparency – personal data is widely available and accessible, particularly, online and through technological developments such as ambient intelligence and cloud computing. Hence, there is a growing difficulty in tracking and controlling how it is used and for what purpose.(v) exercising choice – many services are only provided after sufficient personal data is released, but if important services are denied when individuals are unwilling to supply this data, is there still have a real choice? (vi) assigning accountability – who is ultimately held responsible and where does one go to seek redress?

Multimedia documents contain various data types including text, images, video and audio. Therefore, the preservation of privacy of individuals captured in such documents necessitates de-identifying all their characteristic representations. Indeed, the process will need to be equally effective regardless of whether the recognition attempts are by humans or machines. It can be argued that, in many cases, an additional aspect of the de-identification process should be that of preserving the data utility. For example, the de-identification of individuals in videos captured in nursing homes, for the purpose of monitoring patients, are to conceal the identities of individuals, while maintaining details of the activities, interactions and the manner these have been conducted. Naturally, the Action is also concerned with the robustness of de-identification process against various threats including reversing transformation, manual identification and brute-force verification. Furthermore, the scope of activities includes investigations into reversible de-identification, the analysis of risks involved in such a process, and the security measures for applications requiring the reconstruction of the original data from the de-identified material.

It is therefore a main objective of the Action to bring together scientists and experts from different fields and to foster the creation of a new scientific community for the purpose of dealing with different aspects of de-identification-based privacy preservation. The new community will include the required scientific excellence in various fields, from social and legal sciences to computer science, pattern recognition, computer vision, digital speech and image processing, and biometrics. Indeed, COST offers the most appropriate framework for the proposed activities, as it supports the networking of existing independent EU research teams involved in national research programmes in relevant areas. Moreover, it provides an appropriate platform for the exchange of experiences and results of research in the field of concern, the determination of the way forward, and the coordination of the collective effort. There are no other EU (ESF, ESA,EUREKA, EU Framework Programme) or national funding opportunities to support the activities described above, or to support the creation of the consortium required for the purpose.

It should also be pointed out that, at the moment, there are no European projects in this area. The

Action is envisaged to provide the platform needed for the extension of research efforts in the field by facilitating a complementary Framework project application.

The main benefits expected from the Action can be summarised as follows.

1) Scientific: the goals in this respect can be achieved by promoting collaboration amongst a reasonably wide range of European experts and researchers as well as relevant scientists from non-COST countries. Building on the existing and emerging national research projects in relevant areas and the effective cooperation among partners, the Action is envisaged to deliver considerable advances and novel solutions in the field of concern.

2) Networking of a reasonably wide range of European scientists, as the most important aspect of the COST Action, will facilitate achieving effective progress through sharing and exchanging ideas, solutions, and experiences of the partners. Such an approach will also support the establishment of good practices and standards for the evaluation of the methods and techniques developed. The networking and collaboration of industrial and academic partners with the encouraged involvement of female scientists together with the engagement of Early Stage Researchers (ESRs) will bring to the table a well-balanced and sustainable portfolio of competence.

3)Societal: the outcomes of this Action will provide an effective approach to addressing the growing problem (technical, legal, ethical) of privacy protection in multimedia content, will create opportunities for exploring the added value of de-identified data, and will facilitate the continued capability for the preservation of privacy in multimedia content, as the digital document technology advances.

4)Educational: effective mechanisms are provided to support early stage researchers (ESRs) through Short Term Scientific Missions, summer schools, training programs, invited lecturers, and workshops. It is believed that promoting ESRs is an essential contributor to the sustainable success in the field. A special attention will be given to the involvement of female researchers and, in particular, female ESRs in the Action.

B.2 Current state of knowledge

Research in de-identification was initiated with text-based personal healthcare records (PHRs). The approach in that area involves the removal of a number of specific categories of information from the text file, and replacing them by realistic surrogate information (Golberger et al., 2000; Neamatullah et al. 2008; Sweeney, 1996, 2001).

Early research in image-based de-identification has recommended the use of ad-hoc approaches such as “blurring” and “pixilation” of the image region occupied by a person (Boyle et al., 2000;

Neustaedeter et al., 2005). Such naive methods might prevent a human from recognising subjects in the image, but they cannot thwart recognition systems. An effective approach that subverts naive de-identification methods is called parrot recognition (Newton et al., 2005). The study in (Phillips, 2005) presents an eigenvector-based method, and introduces the privacy-operating characteristic to quantitatively show the trade-off between privacy and security.

In recent years, advances in biometric identification have inspired researchers in the field of de-identification. Examples are the methods termed *k*-Same, *k*-Same-Select algorithms and Model-based *k*-Same for face de-identification (Gross et al., 2009). Despite such studies, numerous problems and challenges still remain to be solved in face de-identification. These include such issues as occlusion, unconstrained head motion, presence of structural components (e.g. glasses, bread), illumination conditions, and most importantly the preservation of data utility (e.g. age, gender and facial expression). Moreover, such characteristics as body silhouette, gait, gesture and soft-biometric markers (e.g. tattoos, birthmarks, scares), hairstyle and dressing style will need to be dealt with effectively, as they carry identity-revealing information (Kumar et al., 2009; Chen et al., 2006; Feng et al. 2008; Lentsoane, 2007). There are additional challenges associated with the de-identification in video sequences (Agrawal, 2011) including the preservation of the naturalness of de-identified moving images.

Other information about individuals, which can be critical to specific aspects of privacy, for example, race, gender, age, will need to be concealed in multimedia content too. The skin marks such as scars and tattoos, and facial marks such as freckles, moles and whitening are also used for identification and will need to be addressed appropriately for the purpose of de-identification (Lee et al. 2008; Niinuma, et al., 2010; Yang et al., 2011).

Likewise, various challenges remain in voice de-identification. This process is based on the principles of voice conversion (Jin et al., 2009), defined as modifying the non-linguistic characteristics of a given utterance without affecting its textual contents. The general approach is to statistically map the original voice to those of a predefined target voice. A challenge here is the generation of mapping functions without the need for parallel data (utterances of the same textual contents) from the source and target speakers. Another challenge is the preservation of intelligibility of the spoken material. Additionally, the de-identified voices should still be sufficiently distinguishable. These are non-trivial issues and addressing them requires extensive investigations.

Another important facet of the Action is reversible de-identification. Reversible de-identification algorithms with an encryption key are a possible approach towards balancing privacy and security requirements. Reversible de-identification is commonly used in the protection of personal data in health care (Fraser, Willison, 2009) and biomedical research (The Bioethics Advisory Committee, 2007). However, rather limited progress is achieved in reversible de-identification in video surveillance systems and multimedia documents (Agrawal, 2010). It is worth noting that in such applications, the parameters for reversing transformation should be saved along with the video (or audio). That poses additional risks, despite the use of encryption in the process.

B.3 Reasons for the Action

Owing to the rapid advances in media acquisition and communication technologies and the move towards a globally networked society, the preservation of privacy in multimedia contents arises as an important and urgent challenge.

De-identification, as the process of concealing the identities of individuals captured in a given set of data (text, audio, images, video) for the purpose of protecting their privacy, will provide an effective means for supporting the EU’s Data Protection Directive (95/46/EC) and recent ICO’s (Information Commissioner’s Office) recommendations.

It should be noted that identity information extracted from multimedia documents can be of various forms including (i) physical biometric data (face, iris, ear); (ii) behavioural biometric data (voice, gait, gesture, lip-motion); (iii) soft biometric data (eye colour, height, weight, silhouette, age, gender, race, moles, tattoos, birthmarks, scars); and (iv) non-biometric data (dressing style, hairstyle, speech context, specific social and political context, environment). This indicates that de-identification is an interdisciplinary challenge, involving such scientific areas as image processing, pattern recognition, speech analysis, video tracking and biometrics.

The main reason for the Action is that there is no effective or formal collaboration at the European level in de-identification, reversible de-identification, or in the related technical, legal and ethical aspects of the subject area. It is believed that establishing a COST-based network of relevant European experts, and organisations in this field, will result in the formation of a new interdisciplinary scientific community capable of initiating and leading the efforts required for achieving effective progress in privacy preservation in multimedia documents.

In terms of concrete outcomes, the main expected synergic effects resulting from the Action can be summarised as follows.

- Development of novel de-identification methods for dealing with physical and behavioural biometric identifiers, which are simultaneously present in multimedia contents (e.g. face, iris, ear, voice, lip-motion, silhouette, gait, and so forth).

- Development of novel de-identification methods for privacy protection by removing or concealing simultaneously present soft biometric data in multimedia contents (e.g. eye colour, height, and weight; age, gender and race; silhouette, age, and gender; moles, birthmarks and scars).

- Development of de-identification methods for non-biometric identifiers (e.g. dressing style and/or speech context; specific social and political context, environment).

- Establishing a platform for collaboration with regulatory and standard bodies in order to maximize the efficiency and employability of de-identification and re-identification in multimedia contents and social network sites.

- Establishing a platform for studies of legal, ethical and social aspects of de- and re-identification in multimedia contents and social network sites.

- Establishing a platform for theoretical research which is related to the evaluation of "quality" of de-identification, and the measurement of the level of de-identification.

B.4 Complementarity with other research programmes

This COST Action closely complements the efforts in COST Action IC 1106, which is concerned with Integrating Biometrics and Forensics for Digital Age. As such, collaboration will be sought with Action IC 1106.
Additionally, there are a number of EU projects, whose activities are expected to be complemented by the Action. The following provides a non-exhaustive list of these projects.
• Intelligent Information System Supporting Observation, Searching and Detection for Security of Citizens in Urban Environment (INDECT)
FP7 research project, Initiated by the Polish Platform for Homeland Security- end date: 2013
• Automatic Detection of Abnormal Behaviour and Threats in Crowded Spaces (ADABTS)
FP7 Collaborative project, projected end date: July 2013
• Digital Image and Video Forensics (DIVEFOR)
FP7-PEOPLE - From 2010-06-01 to 2014-05-31
• Visual Analytic Representation of Large Datasets for Enhancing Network Security (VISSENSE)
FP7-ICT, Collaborative project - From 2010-10-01 to 2013-09-30
• Bayesian biometrics for forensics (BBFOR2)

FP7-PEOPLE - From 2010-01-01 to 2013-12-31

- Trusted Biometrics under Spoofing Attacks (Tabula Rasa)

FP7-ICT, Collaborative project - From 2010-11-01 to 2014-04-30

- BASYLIS - moBile, Autonomous and affordable SYstem to increase safety in Large unpredIctableenvironmentS

FP7-SECURITY, Collaborative project -From 2011-05-01 to 2013-04-30

- ADVISE - Advanced Video Surveillance archives search Engine for security applications

FP7-SECURITY, Small or medium-scale focused research project - 2012-03-01 to 2015-02-28

- BEAT - Biometrics Evaluation and Testing

FP7-SECURITY, Small or medium-scale focused research project- From 2012-03-01 to 2016-02-29

- SOCIALPRIVACY - Addressing Privacy Challenges in Social Media

FP7-PEOPLE - From 2012-09-01 to 2015-08-31

- PRACTIS - Privacy - Appraising challenges to technologies and ethics

FP7-SIS, Small or medium-scale focused research project- From 2010-01-01 to 2012-12-31

- SURVEILLE - Surveillance: Ethical Issues, Legal Limitations, and Efficiency

FP7-SECURITY, Small or medium-scale focused research project- From 2012-02-01 to 2015-04-30

- SMART - Scalable Measures for Automated Recognition Technologies

FP7-SECURITY -From 2011-06-01 to 2014-05-31

The distinction between the projects listed above and the Action is that existing projects are primarily concerned with the recognition and identification of a person (or his/her behaviour), while the focus of the Action is de-identification of a person in order to preserve his or her privacy. Such complementary perspectives can indeed be of benefit in a number of subject areas, especially those related to the legal, ethical and social aspects of privacy in the digital age.

C. OBJECTIVES AND BENEFITS

C.1 Aim

The aim of the Action is to facilitate and promote coordinated efforts in automated person de-identification in multimedia content (text, image, audio and video) through the provision of an effective and innovative approach to the integration of relevant European experts, institutions and organisations, as well as non-COST experts. The Action will deliver concrete results of collaborative research based on vibrant partnerships across disciplinary boundaries. The expected deliverables include novel approaches to robust de-identification, based on the development of effective methods and algorithms for concealing (or removing where appropriate) the biometric identifiers as well as soft- and non-biometric features in the given multimedia documents. Moreover, the Action will deliver guidelines and recommendations for the development of standards in order to maximise the efficacy and employability of de-identification. It will provide the required insights and perspectives on social, ethical, legal aspects of privacy, and will facilitate self-sustaining links and cooperation amongst the researchers, the potential end-users, and system integrators.

C.2 Objectives

The main objectives considered for the Action can be summarized as follows.

- To establish mechanisms for sharing knowledge and technology among experts in different (usually complementary) fields related to automated de-identification and reversible de-identification for privacy protection in multimedia contents.

- To determine the classes of biometric/soft biometric/non-biometric identifiers that are normally present in multimedia contents. Special attention will be paid to a combination of identifiers that belong to different classes and appear simultaneously in multimedia documents (e.g., voice and lip-motion; face and gait, dressing and gesture) and methods for dealing with such identifiers.

- To specify approaches to characterising the correspondence between the choice of de-identification method(s) and the given scenarios and environments.

- To provide innovative solutions for concealing, or removal of, identifiers while preserving data utility and/or naturalness (e.g. de-identification of voice and face in a given video document whilst preserving natural movement of lips).

- To investigate reversible de-identification and to provide a thorough analysis of security risks of reversible de-identification.

- To provide a detailed analysis of legal, ethical and social repercussion of reversible/non-reversible de-identification (e.g., repercussion of reversible/non-reversible de-identification on the behaviour of users of social networks such as Facebook, YouTube and Twitter; determination of privacy protection requirements on Internet sites and social networks; and scientific and technical approaches to fulfilling such requirements).

- To establish cooperation with regulatory and standards bodies (IEC, ITU-T, CEN) in preparation of guidelines and recommendations for maximising the efficacy and employability of de-identification (e.g. cooperation with ISO/IEC Joint Tech. Committee).

- To promote and facilitate the transfer of knowledge to all stakeholders (scientific community, end-users, etc.) through workshops, conference special sessions, seminars and publications.

- To initiate innovation in the training of ESRs and end-users by means of training schools (e.g., online and onsite schools and events and STSMs).

C.3 How networking within the Action will yield the objectives?

The process of de-identification for protecting privacy in the multimedia content is a multidisciplinary problem involving such scientific fields as signal processing, image processing, speech processing, pattern recognition, biometrics, video tracking, machine learning, and so forth. This together with the requirement for the consideration of various complementary and associated issues and concerns necessitate close collaboration of participants collectively offering a broad range of expertise in order to achieve the objectives defined in Section C2. The scope of expertise required for this purpose not only includes various technical fields highlighted above, but also such areas as bioethics, ethics, legal and social sciences. The networking facility provided by COST will offer an effective means for fostering collaboration across national borders and also across different subject areas, as required for this Action. It will not only promote exchange and transfer of knowledge, but will also facilitate the development of innovative solutions through collective efforts. The intention in the Action is to consider both the breadth and effectiveness in the exploitation of the networking opportunity offered by COST in order to maximise the benefit.

C.4 Potential impact of the Action

- The cooperative environment induced by networking of scientists, experts and researchers from different (and often complementary) areas, and opportunities created for their effective cooperation will stimulate new directions of research in the field of privacy protection.

- Owing to the interdisciplinary approach to privacy in multimedia content, the Action creates the opportunities for exploring the added value of de-identified data and supports the harmonisation of progress in privacy and security.

- The impact of the Action will indeed extend to approaches in the development of new applications ranging from speech-based services in telephony, through video-based behavioural monitoring in care homes and hospitals, to intelligent surveillance networks in airports and railway stations.

- Given the interdisciplinary nature of the approach to privacy protection, the Action is expected to provide impact on the wider scientific community – new philosophical, social, legal and ethical perspectives on privacy protection in the digital age.

- Guidelines and recommendation for new standards for maximising the efficacy and employability of de-identification and reversible de-identification.

- Definition of new approaches, standards and recommendations for the protection of privacy of vulnerable groups (children, mentally and physically handicapped people) in audio-video surveillance contents, web sites and social networks.

- Novel ideas in the fields of biometric science and technology, forensic science and audio-video surveillance technology.

- The Action will provide continuing education and training framework, especially for ESRs and end-users, who will in turn support the sustainability of the efforts in the future.

C.5 Target groups/end users

The outcomes and results of this Action could be exploited by a wide range of researchers across distinct technical and non-technical disciplines (biometrics, forensics, bioethics, ethics, legal and social disciplines); governmental institutions; companies; international standards organisations; policy makers; stakeholders involved in privacy protection and human rights. This will include all research and governmental institutions as well as companies and organisations dealing with storing, transferring, processing and utilising multimedia data. The target groups/end users also include social media website owners. In the context of audio-video surveillance, there are also such

potential end users as public transport companies, as well as educational institutions for children, i.e. preschool, primary school, and high school.
Small and medium enterprises (SMEs) together with private and national research institutions and laboratories have been directly involved in the preparation of this Action.

D. SCIENTIFIC PROGRAMME

D.1 Scientific focus

The principal focus of the scientific efforts in this Action is effective approaches to “de-identification in multimedia content” for the purpose of “privacy preservation”. This is a challenging task, with a truly interdisciplinary character. In order for the outcomes to be meaningful and of real value, the intended scope of work is sufficiently broad to cover all facets of the task in a holistic fashion. To this end, and in order to achieve the objectives effectively, the structure considered for the work involves dividing the overall scientific activities into four areas as follows.

- De-identification methods for biometric identifiers;
- De-identification methods for soft- and non-biometric identifiers;
- Applications and added value of de-identified data;
- Ethical, bioethical, societal and legal aspects and guidelines for de-identification and reversible de-identification.

De-identification methods for biometric identifiers

In general, there are a number of biometric identifiers that can be used to identify people in the multimedia content. Among these, the most widely used ones are face, voice, silhouette and gait. While there has been some studies in the area of de-identification related to such biometric identifiers (as described in the Background section), these have been disjointed and largely limited. As a result, there still exists a considerable number of challenges and research problems in the field. For instance, in practice, de-identification methods are required to function in unconstrained environments, in which both the localisation and the de-identification of biometric identifiers are much more difficult than in the laboratory or controlled conditions. Furthermore, a challenge of de-identification is to provide the maximum identity protection while preserving the naturalness of the scene, characteristics of the context, and details of the action being performed.

Face is a biometric identifier that is predominately used by humans to identify individuals. Furthermore, the advances in face recognition enable reliable identification from high quality face images. This, in combination with the fact that face can be collected easily from various multimedia sources, in many situations without the knowledge or the consent of the subject, makes the face modality highly relevant for de-identification. While most current research in face de-identification is based on the frontal face images, this is not sufficient for real-world de-identification. In fact, there remain many challenges in de-identification of face images when they are affected by partial occlusion, bad lighting conditions, cluttered scenes and so forth. Indeed, the complete work on face de-identification should encompass various research areas such as reliable face detection, recognition, de-identification and reversible de-identification.

In uncluttered scenes, the body silhouette and gait can be detected reliably for the purpose of de-identification. In practice, however, the multimedia images are captured from real environments, which are mostly unconstrained and unsupervised. The undesired variation in the operating environment in such cases poses a number of challenging problems, which need to be effectively addressed. Additional difficulties with respect to de-identifying silhouette and gait include avoiding the loss of pictorial information, maintaining the naturalness in the given images, and simultaneously operating on multiple physiological and behavioural features present in the multimedia content. These are non-trivial challenges and addressing them requires through investigations.

Another significant modality that can be used effectively by humans and machines for the recognition of individuals is that of voice. In this case, the de-identification process can be used for protecting privacy in multimedia content as well as in purely audio material. The significance of highlighting the latter is due to the introduction of a growing range of speech-based services. These incorporate such operations as voice recording, storage, and transmission, as well as voice-based user authentication for access control over communication networks. A growing requirement for the effective use of a large subclass of such speech-based services is the introduction of reliable voice de-identification as an appropriate means for preserving the confidentiality of users’ identities. The natural approach for this purpose is that based on voice conversion principles. Ideally, this is the process of converting the voice characteristics of a given utterance so that it appears as if it were produced by another speaker (i.e. conversion of a source voice to a target voice). The challenge in this facet of the project is envisaged to be twofold. First, the intelligibility of the spoken material should not be unacceptably degraded by the process of de-identification (voice conversion). Second, for the purpose of privacy and security, it is desirable to consider only a single target voice for the conversion (de-identification) of all the users' voices in a given application. Despite this, the converted (de-identified) users' voices should still be sufficiently distinguishable. This requirement is of particular importance in applications involving remote access control based on voice biometrics.

The above issues are of considerable importance, and will need to be addressed through innovative approaches in order to facilitate an effective realisation of voice de-identification for real-world applications.

De-identification methods for soft- and non-biometric identifiers

Soft biometric identifiers, such as age, gender, race, hair style, skin marks and tattoos can be used to help identify individuals, either in combination with other identifiers or on their own, if sufficient number of them is present. This opens up a need for novel investigations into de-identification methods aimed at soft-biometric identifiers.

This Action will help to define a research framework and guidelines for the de-identification of soft-biometric traits and also for reversible de-identification.

Hand gestures have traditionally been recognised for human-computer interaction, suspicious behaviour detection and sign language interpretation but not identification. However sequences of gestures are a valid biometric identifier. Therefore, gesture de-identification is considered another important facet of investigations within the Action.

Non-biometric identifiers such as hairstyle and clothing style are not yet sufficiently explored in the context of person identification, but they are potentially non-biometric identifiers. As such, they will form a facet of research in this Action.

Applications and added value of de-identified data

The Action will focus on a variety of applications ranging from speech-based services in telephony to video-based behavioural monitoring in care homes and law enforcement in airports. The scope of the work will include the study of potential benefits as well as the deployment challenges and the issues in each case. Special attention will be devoted to methods for privacy protection of vulnerable groups (children, mentally and physically handicapped people) in audio-video surveillance content.

Considering the amount of personal identifiable data that can be found on Internet sites, predominately social networks (Facebook, YouTube, Twitter etc.), special attention needs to be given to develop de-identification technologies for these kinds of applications. Additionally, there are various other Internet applications (besides the social networks) with a growing need for privacy protection. A clear example is “Google Street View” and the privacy concerns surrounding it. This Action will help to identify such applications and the corresponding privacy protection requirements and will propose the scientific and technical approaches to fulfilling those requirements.

Other notable potential application areas are in public transportation, preschool and school educational institutions for children (in context of audio-video surveillance)

Ethical, bioethical, societal and legal aspects and guidelines for de-identification and reversible de-identification

The Action will study legal, ethical, bioethical and social aspects of de-identification and reversible de-identification. The study will include the following three main areas: (i) impact of de-identification and reversible de-identification on fundamental human rights; (ii) impact on privacy and data protection; (iii) impact on vulnerable and disadvantaged groups.

The Action will study the impact of technical aspects in the above areas. This study will take into account both existing regulations such as the 1995 EU Data Protection Directive (95/46/EC), its 2008 review by the Information Commissioner’s Office (ICO), and the Charter of Fundamental Rights by the European Union (COM-2010 573 final, adopted by the Commission on 19 October 2010). Additionally, the proposed study will take in to consideration the rapid technological changes, as well as the move towards a global networked society.

In summary, the task is expected to facilitate the maximisation of the efficacy and employability of de-identification through the provision of recommendations and guidelines.

D.2 Scientific work plan methods and means

The scientific work plan is designed with the intention to address the key challenges identified and specified in Section B, as well as to achieve the objectives listed in Section C. The approach considered for the initial stage will involve due reference to the existing literature relating to (i) privacy and privacy protection; (ii) the state-of-the-art in automatic biometric identification; and (iii) soft/non-biometric identifiers. It is believed that the expertise and experience in automatic biometric identification will prove highly beneficial in the development of innovative solutions in the field of de-identification.

Using the outcomes of the above phase of operation, the focus will then be directed on approaches to detecting and localising personal identifiers in multimedia documents. In this respect, there will be particular attention on data conditions in real applications. The results in this part will be used for the purpose of the main facet of investigations, which is concerned with the development of effective methods for de-identification. These investigations will be coupled with research into approaches to maintaining the naturalness and utility of de-identified data so that the overall outcomes are still meaningful and offer as much value as the original data for different applications considered.

As a natural extension of the above investigations, the next stage of activities will be mostly concerned with research into methods for reversible de-identification. This is for particular applications in which the capability for the restoration of original data is a requirement (or just permissible). The investigation in this area will be supported by a thorough analysis of the security and privacy risks involved, and by complementary research into innovative cryptographic approaches for securing the data restoration keys.

For the purpose of evaluation, the required framework and procedures will be appropriately defined. This is, in particular, related to (i) De-identification methods for biometric identifiers, and (ii) De-identification methods for soft- and non-biometric identifiers. This facet of work requires the introduction of properly validated metrics for the purpose of evaluating the degree of de-identification achieved in multimedia content. Another factor considered in the study is the fact that the effectiveness evaluation should be conducted with respect to identification attempts by both machines and humans.

The Action will investigate and propose solutions for different scenarios and applications in which the introduction of de-identification technologies are considered beneficial. This will include intelligent, multi-sensor surveillance systems applied in transportation, educational institutions, healthcare, airport, and so forth. Another application area is that of online social networks and other Internet services. The added value of de-identification in such cases is the provision of secure storage, retrieval, offline analysis, as well as exchange of the de-identified data between institutions. The efforts in these areas will form the focus of activities in the task entitled (iii) Applications and added value of de-identified data.

Through coordinated activities amongst participants from both technical and non-technical fields, the Action is expected to provide impact on the wider scientific community. This will encompass legal, ethical, bioethical and societal aspects of the de-identification and reversible de-identification. The Action will propose guidelines and recommendations that may have impact on the standards related to privacy, data protection and human rights. The Action will actively seek collaboration with regulatory and standard bodies. This aspect of the work plan is delivered through the task entitled (iv) Ethical, bioethical, societal and legal aspects and guidelines for de-identification and reversible de-identification.

E. ORGANISATION

E.1 Coordination and organisation

The Management Committee (MC) will elect the Action Chairperson and Vice Chairperson at the kick-off meeting. The MC will meet at least twice a year in order to monitor and coordinate the activities, and monitor the progress of the Action. The MC will foster the connections with the complementary Actions, as well as other projects and stakeholders. The members of the MC should be involved in research and development activities related to at least one of the main scientific areas of the Action. At least three MC members will be nominated and selected as the Short Term Scientific Mission (STSM) Committee. The STSM Committee will assess and approve the applications, as well as evaluate the results of the STSMs. All decisions of the STSM Committee will be reported to the next MC meeting.

According to the research areas described in Section D, the Action will consist of the four working groups (WGs) defined in Section E.2. Activities and networking of WG members will be led and represented by the corresponding WG coordinators, who also act the MC liaisons. The MC members will nominate and elect the coordinator for each WG.

Each WG coordinator will regularly report on the progress and challenges in his/her WG. The periodical reports of the WG coordinators, collectively inform the definition and review of the direction and nature of efforts within the Action.

The MC members will also act as the representatives of their respective countries, and are involved in the national research projects related to the Action. The coordination of national research efforts within different member countries will be supported through the organisation of international conferences and workshops, STSMs, Action website, online and onsite training schools, events for ESRs and joint PhD programmes.

A special team will be selected to create and maintain the Action website. The website will be regularly updated during the entire duration of the Action. The website team will have administrator privileges, but all participants will be offered the opportunity to provide content for publication on the website. The website will have a common section as well as separate sections for individual

WGs.

E.2 Working Groups

The Action will consist of four WGs, each being responsible for one of the research areas defined in Section D:

WG1: De-identification methods for biometric identifiers

WG2: De-identification methods for soft- and non-biometric identifiers

WG3: Applications and added value of de-identified data

WG4: Ethical, bioethical, societal and legal aspects and guidelines for de-identification and reversible de-identification

Their operational organisation is as follows:

WG1: De-identification methods for biometric identifiers

and

WG2: De-identification methods for soft- and non-biometric identifiers

WG1 will cover research and development (R&D) activities related to physiological and behavioural biometric identifiers. The main physiological identifiers in the multimedia contents are face, ear and iris. The behavioural identifiers include voice, gait, gesture, lip movement and signature

WG2 will cover R&D activities related to soft- and non-biometric identifiers. Soft-biometric identifiers covered by this WG include age, gender, ethnicity, height, weight, skin marks etc. Non-biometric identifiers include hairstyle, clothing style, text and environmental context.

The activities in WG1 & WG2 are structured appropriately to include the following key areas.

- Previous approaches to, and the main challenges in multimedia de-identification.
- Definition and classification of biometric/soft biometric/non-biometric identifiers in the multimedia content.
- Real-time, robust methods for identifier detection and localisation.
- Innovative methods for de-identification and reversible de-identification.
- Preservation of data utility and naturalness in de-identification.
- Procedures for the evaluation of de-identification methods.

- Security risks associated with reversible de-identification.

Due to the nature of multimedia content in which identifiers from different classes are simultaneously present, the cooperation of the above WGs are necessary in order to maximise progress.

WG3: Applications and added value of de-identified data

This WG will cover a variety of applications including

- Law enforcement in
  - transportation
  - private surveillance systems
- Video-based behavioural monitoring in
  - schools and other educational institutions
  - care homes and hospitals
- Speech-based services in telephony and online
- Text-based medical record in healthcare
- Online social networks and other Internet services

WG3 will also cover the assessment of added-value of the de-identified data through the possibility of secure storage, retrieval, offline analysis, as well as the exchange of de-identified data between institutions. Special attention will be devoted to methods for privacy protection of vulnerable groups (children, mentally and physically handicapped people) in audio-video surveillance content.

WG4: Ethical, bioethical, societal and legal aspects and guidelines for de-identification and reversible de-identification

Activities will involve collaboration with regulatory and standards bodies. The areas of concern will include:

- Existing policies and regulations;
- New philosophical, societal and ethical perspectives on privacy protection in the digital age;
- Guidelines and recommendations that may facilitate and support the standards;
- Assessment of impact of de-identification on privacy, data protection and human rights.

E.3 Liaison and interaction with other research programmes

The Action will actively seek to liaise with other projects in relevant fields. Working liaison with complementary COST Actions will, in general, be achieved through consultation with the corresponding COST Action Management Committees.

An effective collaboration with other current EU and national projects can be achieved by drawing the interest of researchers involved in these projects to this COST Action. Examples of such projects include COST Action 1106: Integrating Biometrics and Forensics for the Digital Age, EU FP7 “Digital Image and Video Forensics”, EU FP7 SMART “Scalable Measures for Automated Recognition Technologies”, EU FP7 RESPECT “Rules, Expectations & Security through Privacy-Enhanced Convenient Technologies”, EU FP7 TABULA RASA “Trusted Biometrics under Spoofing Attacks”, to name a few.

One form of collaboration will be inviting experts from other projects to participate in the thematic workshops and WG meetings of this Action.

E.4 Gender balance and involvement of early-stage researchers

The Action will also be committed to considerably involve early-stage researchers (ESRs). This item will also be placed as a standard item on the agenda for the MC meetings. In order to further facilitate this objective, effective mechanisms will be provided to support ESRs through STSMs, summer schools, training programs, invited lectures, and workshops. It is believed that promoting ESRs is an essential contributor to the sustainable success in the field.

F. TIMETABLE

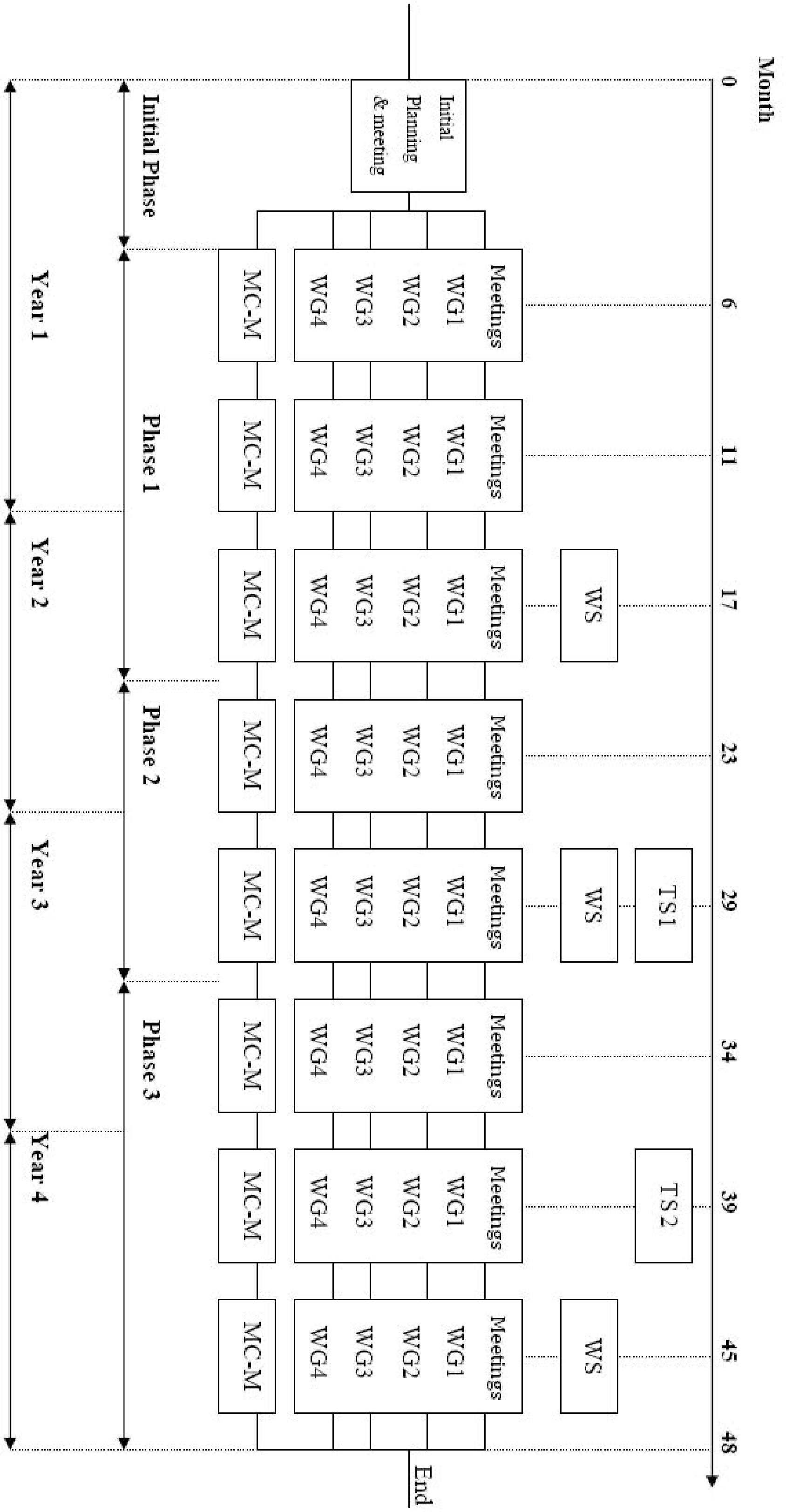
The duration of this Action is 4 years.

The Action is organized into an initial phase and the three subsequent phases. Table 1 depicts the duration of each phase together with the description of activities during individual phases.

Table 1. Timetable for the Action

Activity	*Duration*
Initial phase Election of Chair, Vice-chair, budget holder, Working Group Coordinators, STSM Committee Members and initial planning; Setting up of the Action web site.	4 months
Phase 1 Coordinated networking of scientific activities in the areas of de-identification, reversible de-identification and privacy protection in WGs 1-4; Organising the first Action Workshop; Creating liaisons with the other COST Actions; Fostering and activation of inter-partner STSM visits; Establishing links with appropriate organisations; Updating the Action web site.	16 months
Phase 2 Coordinated networking of scientific activities in the areas of de-identification, reversible de-identification and privacy protection in WGs 1-4.; Organising the second Action Workshop; Monitoring and arranging networking inter-partner STSM visits; Organizing the first Training School; Liaison with other Actions; Presenting scientific papers at conferences; Updating the Action web site.	12 months
Phase 3 Coordinated networking of scientific activities in the areas of de-identification, reversible de-identification and privacy protection in WGs 1-4.; Monitoring and arranging networking inter-partner STSM visits; Organising the final Action Workshop; Organizing the second Training School; Presenting scientific papers at conferences; Updating the Action web site; Preparation of the final report of the Action.	16 months

Figure 1. Time plan for the Action. WG: Working Group; MC-M: Management Committee Meeting; WS: Workshop; TS: Training School.



G. ECONOMIC DIMENSION

The following COST countries have actively participated in the preparation of the Action or otherwise indicated their interest: CY, DE, DK, EL, ES, FI, FR, HR, IT, MT, PL, PT, SI, UK. On the basis of national estimates, the economic dimension of the activities to be carried out under the Action has been estimated at 56 Million € for the total duration of the Action. This estimate is valid under the assumption that all the countries mentioned above but no other countries will participate in the Action. Any departure from this will change the total cost accordingly.

H. DISSEMINATION PLAN

H.1 Who?

The main target audiences for the dissemination will be:

- Wide range of researchers across distinct technical and non-technical disciplines (biometrics, forensics, bioethics, ethics, legal and social disciplines);
- Governmental institutions (concerned specifically with security and privacy protection);
- Law enforcement agencies;
- Service providers in the public and private domains;
- International standard organisations and policy makers in the field of privacy protection;
- Research and governmental institutions as well as companies and organisations dealing with storing, transferring, processing and utilising multimedia data (public transportation companies, preschool and school educational institutions etc.);
- Social media websites;
- PhD candidates and early stage researchers (ESRs) working in the fields of biometrics, de-identification and reversible de-identification in multimedia contents;
- Other EU projects in the related fields.

H.2 What?

The approach to dissemination will include all the elements known to be effective such as:

- Provision on the Action website of “interim progress reports”, “state of the art reports” and “case studies”;
- Creation of an internet forum and a mailing list;
- Workshops and special sessions at international scientific conferences;
- Training school on the main topics of concern, i.e. de-identification, reversible de-identification and privacy protection;
- Scientific papers in peer-reviewed scientific and technical journals;
- Non-technical publications related to ethical, bioethical and legal issues of de-identification; and
- Publication of guidelines and recommendations.

The outcomes of the Action will be incorporated into the existing and future joint biometrics- and de-identification research and educational activities and also for proposing joint PhD programmes at participating academic institutions.

H.3 How?

The dissemination of information and findings will be planned and managed by the Management Committee and/or by a special team formed for this purpose.

Due to the interdisciplinary character of the Action, the dissemination will be targeted to both technical and non-technical audiences, and will take place at several levels. These include the Action website; workshops, special sessions at conferences; training schools and STSMs aimed to the ESRs and researchers; joint publications in journals and proceedings of international conferences; non-technical publications; guidelines and recommendations. Thematic meetings with the end-users and other stakeholders are also planned, as well as meetings with non-technical experts covering ethical, bioethical and legal aspects of the Action.

In order to ensure that the Action website will serve the dissemination purposes effectively as well as facilitating communication, it will be designed to include the following information:

- A list of the official members and all other participants, giving their names, organisations, postal and e-mail addresses as well as telephone and fax numbers. In order to further facilitate communication, a group e-mail address will also be issued.
- Structure and activities of the Action.
- Previous and forthcoming events, including MC meetings and workshops.
- Appropriate technical reports and experimental results.
- Special reports and application notes.
- Minutes of MC meetings.
- Proceedings of the workshops run by the Action.
- Links to other appropriate websites. For example other organisations, COST Actions and European projects involved in a related field.