THE MISSING
the right to know

The Missing:
Action to resolve the problem of people unaccounted for as a result of armed conflict or internal violence and to assist their families

The legal protection of personal data & human remains

Electronic Workshop
02.04.2002 - 06.05.2002

Final report and outcome

Mission statement

The aim is to heighten awareness among governments, the military, international and national organizations – including the worldwide Red Cross and Red Crescent network – and the general public about the tragedy of people unaccounted for as a result of armed conflict or internal violence and about the anguish of their families

by creating and making available tools for action and communication

in order to ensure accountability on the part of the authorities responsible for resolving the problem of missing people, to better assist the families and to prevent further disappearances.

ICRC

Table of content

1. Introduction

1.1 Introduction to the process "The Missing"

This workshop is part of an interactive process of reflection launched by the International Committee of the Red Cross (ICRC) on the tragedy of people unaccounted for as a result of armed conflict or internal violence.

Uncertainty as to the fate of relatives is a harsh reality for countless families in all situations of armed conflict or internal violence, one that often continues for many years. Not only is this deeply distressing for the families, it can also hamper efforts aimed at achieving reconciliation and an enduring peace by contributing to further outbreaks of violence.

Accordingly, the ICRC's objective in launching this process, in cooperation with all those involved in dealing with the issue, is to:

- review all methods that could be employed to prevent disappearances in situations of armed conflict or internal violence more effectively, and respond to the needs of families that have lost contact with their loved ones;
- agree on common and complementary recommendations and operational practices with all those working to prevent disappearances, and respond appropriately when people are unaccounted for in a situation of armed conflict or internal violence;
- position this concern higher on the agendas of government authorities, the United Nations and non-governmental organizations.

The process is being conducted in two stages.

During the first stage, studies are being conducted by a number of research centers and workshops are being organized that bring together governmental and/or non-governmental experts on topics relating to the issue of disappearances. The studies and workshops are intended to help clarify needs and the means of meeting them and to define recommendations and the best operational practices to be implemented. The present workshop is one of those events, all of which are listed below:

- 2 electronic workshops:
  - Human remains & forensic sciences: preparatory electronic workshop,
  - The legal protection of personal data & human remains,
- 3 studies:
  - Mourning process & commemoration,
  - Overcoming the tensions between family needs and judicial procedures,
  - Study on existing mechanisms to clarify the fate of people unaccounted for,
- 6 workshops taking place in the following order:
  - Member of armed forces / armed groups: identification, family news, killed in action, prevention,
  - Human remains: Law, politics & ethics,
  - Support to families of people unaccounted for,
  - Human remains: management of remains and of information on the dead,
  - Means to prevent disappearances & to process missing cases,
  - Mechanisms to solve issues on people unaccounted for.

The preparatory phase of each workshop comprises:

- the establishment of reference documents based on international humanitarian law and human rights, and relevant lessons or experiences from past and present situations of armed conflict or violence;
- written contributions from experts invited to participate in the workshop concerned, such as senior military officers, senior government officials, historians, lawyers, medical, psychology or forensic specialists and academics.

Documents are made available to the participants via a dedicated Extranet that allows all of them to follow the entire process.

At the end of each workshop, the outcome is summarized by the ICRC and posted on the Extranet. Individual opinions are not recorded; neither the participants nor their organizations bear responsibility for the summary.

In addition, the final report of the workshop, including the outcome, experts' contributions and the ICRC preparatory documents, will be prepared and subsequently published in English and French.

During the second stage, the ICRC will convene an international conference of the experts who took part in the workshops and of any other interested parties. The conference will be held in Geneva from 19 to 21 February 2003.

The results of the first stage will be submitted to the conference participants in the form of a document which will be compiled by the ICRC and which will contain all recommendations and best practices, for adoption by the international conference in February 2003. This document will take into account the outcome of all events; obviously, there will be some overlap between events, as the same topic may be dealt with from different perspectives.

The ICRC hopes that the conference results will be directly useful both to:

- individuals and organizations working in the political, humanitarian and human rights fields and active on the ground in situations of armed conflict or internal violence, and
- governments involved in developing international law and preventing or resolving conflicts, especially within the framework of the United Nations, for example through its Human Rights Commission, or within the International Red Cross and Red Crescent Movement, for example through the International Conference of the Red Cross and Red Crescent.

1.2 The legal protection of personal data & human remains

Aim of the electronic workshop

The aim of the workshop was to define basic general principles regarding the legal protection of personal data and the identification of persons unaccounted for which could be upheld worldwide, in particular during and after situations of armed conflict or internal violence, in order to ensure best practices from all those involved in resolving issues related to missing persons.

- It is clear that in such situations, domestic law, including rules on the protection of personal data if they exist, generally remains applicable. In situations of armed conflict or internal violence, however, it might be difficult to ascertain what the domestic rules are.
- Also, in some situations, domestic rules may simply not exist or not address a particular issue (for instance, taking and analysing DNA samples), it might not be clear to whom they are applicable or they may not be applicable in practice.
- Furthermore, government agencies might not be in a position to enforce the law, public services might be disorganized and a number of international or foreign agencies or institutions might be involved.

In practice, in several contexts there has been no proper legal framework, in terms of the protection of privacy and personal data, for the search for the missing and the identification of human remains.

The workshop's purpose was therefore to draft the basic principles to be followed in any situation and by all the entities concerned, and thus avoid harmful consequences and mismanagement. It is hoped that these principles will eventually be applied by local, foreign and international bodies or agencies, either public and private, whatever their formal status or the special immunities or privileges they may enjoy under domestic or international law. They are limited, however, to the substantive aspects of the protection of personal data and the identification of persons unaccounted for. They do not include the technical or procedural aspects of data processing, DNA analysis or exhumation.

The process

An initial document containing draft principles was drawn up by the ICRC on the basis of the main international texts and a selection of domestic laws and regulations on the subject. That document was then submitted to a team of external legal experts for two rounds of comments through the electronic workshop. The participating legal experts were:

- Ms Alejandra Gils Carbó, Prosecutor and Data Protection Expert, Attorney General's Office, Argentina;
- Mr Douwe Korff, legal consultant (human rights and data protection), United Kingdom;
- Mr Eugene Oscapella, legal consultant (data protection in the medical and genetic fields), Canada;
- Mr Kosmas Tsiraktsopulos, Office of the Federal Data Protection Commissioner, Switzerland.

The initial document was redrafted twice to take account of the comments and suggestions made by the participating legal experts.

The ICRC is the author of the following sections. They do not necessarily reflect the views of the experts who were consulted in the course of the workshop.

2. Outcome: Commonly accepted principles

2.1 Protection of personal data: commonly accepted principles

a. Quality of data

Principle 1 **"Personal data" means any information relating to an identified or identifiable individual.**

In most international and domestic texts, the definition of "personal data" is very broad. The Council of Europe *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981)* (the CoE Convention) defines "personal data" as "any information relating to an identified or identifiable individual". This definition is broad enough to include all biometric data, including medical information and genetic information.

An "identifiable" person is a person who can be identified, directly or indirectly. It does not mean that the data has to be linked to a named person: data on unnamed living persons (such as the fingerprints of a suspect in a police station who refuses to give his name, or medical data on an accident victim admitted to hospital while unconscious) are also "personal". The definition is more complex when it comes to semi-identifiable data, such as *pseudonymized* data or data which could be linked to an identified person by some people in certain circumstances but not by others in other circumstances. Some laws regard such data as always personal and subject to data protection rules (even if processed by someone without access to the identifying "key"), although the application of the rules may be less stringent. Others regard such data as personal only with regard to someone who does have access to the "key", but hold that other general rules on the processing of encoded data may be applicable; still others fully exempt such data from all legal restraints.

More qualitative data, such as lifestyles, activities, participation at certain events, memberships, etc., are covered by the term "personal data", as long as they relate to an identified or identifiable individual. For instance, the Russian *Law on Information* defines personal data as "reports on facts, events, lifestyles of citizens which allow for the identification of individual citizens". Other domestic laws have similarly broad definitions. The collection, use and disclosure of this type of data are thus subject to the same principles as any other personal data. They are also subject to the particular safeguards for the collection and processing of sensitive data, if such information is considered sensitive or if it could lead to the disclosure of other sensitive individual information.

Some domestic laws apply to the protection of the personal data of a living individual only (e.g., the United Kingdom's *Data Protection Act*). Hence, data relating to dead persons are not subject to data protection rules. Others lay down specific rules in certain circumstances. The French *Law on Personal Records* allows the processing of data on deceased persons for purposes of medical research unless the person expressly opposed such processing while still alive. Still others provide that personal data about a person who has been dead for a period of time is no longer considered personal information for certain purposes. Under the Canadian federal *Privacy Act*, which governs the personal data-handling practices of federal institutions, information about a person who has been dead for more than 20 years is no longer considered "personal information" when applying certain sections of the Act. Thus, for example, the rules in the Act preventing the use of personal information for purposes inconsistent with the purpose of its original collection, and those limiting disclosure of such information, do not apply to such information. This may have implications for the use and disclosure of information about individuals who are known to be dead, but whose remains have not been located. A judicial order or declaration recognizing a presumed death would allow information about the person to be used to help locate the person or the person's remains. The proceedings and the period of time required for a person to be presumed dead vary from one Canadian province to another.

"sensitive data"

Most domestic laws include a category of personal data considered to be sensitive and subject to specific safeguards. There is no standard definition of "sensitive data". This category of data is usually not precisely defined but appears as a list of types of data subject to specific protection or as prohibited grounds of discrimination.

Data on racial or ethnic origin, political opinions, religious, philosophical and other beliefs, health or sexual life, criminal convictions, and membership in an association or trade union are included in most domestic and international texts as sensitive data. The Chilean *Law on the protection of personal data*, for instance, defines sensitive data as personal data related to the physical or moral characteristics of persons or facts or circumstances of their private or intimate lives, such as personal habits, racial origin, ideologies or political opinions, religious beliefs or convictions, physical or psychological health conditions or sexual life. In other laws, sensitive data appears as a closed list.

While these types of personal data are nearly always considered as sensitive, other types of data can also fall into that category. Nearly any personal data may be considered sensitive in certain circumstances. Rather than limiting sensitive data to a list of prohibited grounds of discrimination, sensitive data could be defined as personal information that can be used to the detriment of the individual to which it relates. Sensitive data are also data from which sensitive personal information can be inferred or which can lead to the disclosure of such information.

Most personal data collected for the purpose of establishing the identity, whereabouts and fate of missing persons would fall into the category of sensitive data.

UN Guidelines	CoE Convention (art. 6)	CoE (CM) R 87 (15)	European Community Directive 95/46/EC	Argentina	Chile	France	Russian Federation	Switzerland	United Kingdom
racial or ethnic origin, color	**racial origin**	**racial origin**	**racial or ethnic origin**	**racial or ethnic origin**	**racial origin**	**racial origin**	**race, nationality, language**	**race**	**racial or ethnic origin**
political opinions	**political opinions**	**political opinions**	**political opinions**	**political opinions**	**ideologies or political opinions**	**political opinions**		**political opinions or activities**	**political opinions**
religious, philosophical and other beliefs	**religious or other beliefs**	**religious convictions**	**religious or philosophical beliefs**	**religious, philosophical or moral convictions**	**religious beliefs or convictions**	**religious beliefs**	**religion**	**religious, philosophical opinions or activities**	**religious or other beliefs**
sex life	**health or sexual life**	**sexual behavior**	**health or sex life**	**health or sexual life**	**physical or psychological health, sexual life**			**health or intimate sphere**	**physical or mental health, sexual life**
	criminal convictions			***** (see Art. 7(4)**				**criminal or administrative prosecutions or penalties**	**commission of an offence or alleged commission of an offence, and proceedings and sentences**
							social origin	**social welfare benefits**	
membership in an association or a trade union		**belonging to particular movements or organizations**	**trade union membership**	**membership in a trade union**		**membership in a trade union**	**party membership**	**opinions on or activities in a trade union**	**membership in an association or a trade union**

"medical data" (or "health information")

"Medical data" refers to all personal data concerning the health of an individual. It also refers to data which have a clear and close link with health, including genetic data. The Canadian *Personal Information Protection and Electronic Documents Act*, which applies to commercial undertakings operating under federal jurisdiction, defines "personal health information" as "with respect to an individual, whether living or deceased, [...]

- information concerning the physical or mental health of the individual;
- information concerning any health service provided to the individual;
- information concerning the donation by the individual of any body part or any bodily substance of the individual or information derived from the testing or examination of a body part or bodily substance of the individual;
- information that is collected in the course of providing health services to the individual; or
- information that is collected incidentally to the provision of health services to the individual".

Health information is considered as sensitive data in most domestic and international texts, and is subject to specific rules of disclosure. Although generally not specifically provided for in legal texts, there is a trend to consider DNA data as sensitive data as well, or as a special category of data subject to more restrictive data protection rules.

b. Collection and processing of personal data

International and domestic rules have been adopted on the protection of personal data in order to protect individuals against encroachments on their right to privacy by the public authorities or private bodies. In the context of the search for missing persons, data are collected, processed and disclosed primarily for the benefit of the individual to whom they relate, and not in the interests of third parties or in the public interest.

Principle 2
Personal data shall be collected and processed fairly and lawfully.

It is a recognized principle in both international (*United Nations Guidelines for the Regulation of Computerized Personal Data Files* (1990) (UN Guidelines), the CoE Convention, the OECD *Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (1980)* (OECD Guidelines)) and domestic texts (Argentina, Canada, Chile, France, Switzerland) that personal data should be collected and processed fairly and lawfully.

The term "processing" generally includes any operation or set of operations performed on personal data. *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data* (EC Directive 95/46/EC) defines "processing" as "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction" (see also the United Kingdom *Data Protection Act 1998* and the Argentine *Personal Data Protection Act*).

Whether or not the method of collection is fair depends in part on the type of data to be collected and its use (e.g., data used for law enforcement purposes *vs* data collected for social welfare entitlements). The method should not be deceptive, fraudulent or contrary to the law. This principle is intended to ensure that individuals are not mislead or deceived about the purpose for which the data is being collected. It also implies that consent with respect to collection must not be obtained through deception.

Where data is not obtained directly from the person to whom it relates, the data controller, i.e. the person, authority, agency or any other body which determines the purpose for which the data is processed and how, will not always be in a position to attest or verify that the information was obtained by fair and lawful methods by intermediaries who are not its agents. This must be accepted as a persistent difficulty when attempting to locate missing individuals. The problem is akin to that faced by police conducting investigations. They themselves may be subject to rules requiring fairness in acquiring information for their investigations (rules on electronic surveillance, for example), but if they acquire information from another source, they are not obliged to ignore that information. The same logic may apply in the case of missing persons. Given that the overriding and valid goal is to locate such individuals, a controller collecting information that may have been acquired improperly by others should nonetheless be allowed to collect the information, as long as he was in no way implicated in that improper collection and did not encourage or tolerate such collection. He must be particularly alert, however, to the fact that the information may be inaccurate.

Principle 3
The consent of the individual is required for the collection and use of personal data, except where inappropriate.

Most international and domestic texts provide that the consent of the individual should generally be obtained before data is collected. Some do not seem to require consent, but provide for a right to oppose the processing of personal data (France). Some laws specifically allow consent to be withdrawn, subject to legal restrictions and reasonable notice (Argentina, Canada).

Domestic legislation (Canada, Argentina, Switzerland) prescribes that consent must be free and informed. For example, the Canadian *Personal Information Protection and Electronic Documents Act* states that the principle requires "knowledge and consent", i.e. a reasonable effort has to be made to ensure that the individual is advised of the purposes for which the information will be used and the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed. The Argentine *Personal Data Protection Act* provides that the following information should be furnished to the person to whom the collected information relates:

- the purpose for which the information was collected and for whom it is intended, including its transfer to any third party;
- the existence of archives, registers, databases that use personal data;
- the obligatory or facultative nature of the information requested;
- the possible consequences of not providing the data or of providing inaccurate data;
- the individual's possibility to exercise a right of access to, to rectify or to suppress personal data.

Similar duties of information may be found in other legislation (e.g., France).

The way consent is sought may vary depending on the circumstances and the type of information collected. Implied consent may be considered reasonable in some cases, for instance when the person provides the information of his own volition for a specific purpose. The reasonable expectations of the individual may also be taken into account. The circumstances in which information may be collected without the consent or knowledge of the individual are generally stipulated in particular legal provisions and are subject to specific requirements. These circumstances are usually related to the protection of a public interest (maintenance of public order and criminal investigations, communication of data between government agencies, protection of public health), or to cases in which the collection of information is clearly in the interests of the individual concerned and consent cannot be obtained in a timely way (Argentina, Canada, Germany).

Given the nature of the information relative to missing persons, obtaining the consent of subjects on whom information is collected and processed may be inappropriate or impossible. The collection of personal data for the purpose of locating a missing person can, however, be considered to be clearly in the interests of that person. Hence, personal information to be used for that purpose could be collected without the individual's consent or knowledge.

In circumstances where data is collected without consent, the individual nevertheless retains the right to be informed of the existence, use and disclosure of his or her personal information. *Recommendation (87) 15* of the Council of Europe Committee of Ministers regulating the use of personal data in the police sector (CoM Recommendation) states, for instance, that unless the data is deleted, the individual should be informed, where practicable, that information is being held about him as soon as the object of the police activities is no longer likely to be prejudiced (§ 2.2).

When personal information is collected from another person or from a third party without the consent or knowledge of the person to whom the information relates, the person should be informed as soon as practicable of the existence of the personal information concerning him. The principle of consent implies that a person has a right to object to the processing of personal data concerning him when he is informed of the collection and processing. That information should then be excluded from further processing if there are no overriding interests against such discontinuation.

Principle 4
The collection and processing of personal data shall be limited to that which is necessary for the purpose identified at the time of collection, or beforehand.

A basic principle of the collection of personal information is that it cannot be done indiscriminately, for some undetermined purpose, or for a purpose to be determined in the future only. The principle of purpose specification is recognized in international (UN Guidelines, CoE Convention, OECD Guidelines) and domestic texts (Argentina, Canada, United Kingdom).

The purpose of the collection must be lawful and appropriate. There should be a reasonable link between the mission or the activities of the organization and the purpose of the data collection. The Canadian *Privacy Act* states that "no personal information shall be collected by a government institution unless it relates directly to an operating program or activity of the institution". Similarly, the Canadian *Personal Information Protection Act* provides that "an organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances".

The principle of purpose specification also entails that the amount and type of information collected and stored should be limited to what is necessary to fulfill the specified purpose. Data collection and storage should not be excessive in relation to the purpose for which the data are processed. The use of collected personal information should similarly be limited to the fulfillment of the specified purpose. Personal data cannot be used for other purposes, or for purposes inconsistent with the purpose for which they were collected and processed.

In accordance with the principle of informed consent, the purpose must be disclosed to the person relative to whom the information is collected. It should also be disclosed to any third party providing information on that person, since the third party should be able to ascertain whether the use and transfer of the data is consistent with data protection principles. When personal data is collected from a person other than the person to whom that data relates, that person should be informed of the purpose of the collection, whether response is voluntary or required by law, any possible consequences of refusing to respond, and that the individual to whom the information pertains has rights of access to and protection of the personal data.

The principle is *a priori* applicable to the collection, use and storage of all personal data. Any exception to this principle should be clearly stated in the law. Article 9 of the CoE Convention allows for a derogation to this principle if it constitutes "a necessary measure in a democratic society in the interests of [...] protecting State security, public safety, [...] or the suppression of criminal offences; [or] protecting the data subject or the rights and freedoms of others". In accordance with this principle, it is for instance reaffirmed in the CoM Recommendation that the collection of personal data for police purposes should be limited to such as is necessary for the prevention of a real danger or the suppression of a specific criminal offence.

In the context of the search for missing persons, respect for the predetermined purpose for which the personal data was collected and processed is particularly important since many exceptions may be invoked to the general rules of data protection on the grounds that they are in the vital interests of the missing person. The primary purposes of data collection in relation to persons unaccounted for are:

- to establish the identity, location, conditions and fate of living persons who are unaccounted for;
- to establish the identity, location, conditions and fate of deceased persons who are unaccounted for;
- to give families information on the whereabouts, conditions and fate of their missing relatives.

For those purposes, the data collected might include:

- for living missing persons:
  - administrative data (name, place of residence, etc.);
  - qualitative data (occupational details, activities, last known whereabouts, etc.);
  - biometric data (sex, age, description, etc.); DNA information is not generally collected for living persons who are unaccounted for;
- for deceased and unidentified persons:
  - administrative data (name, place of residence, etc.);
  - qualitative data (occupation details, activities, last known whereabouts, etc.);
  - biometric data (sex, age, description, etc.), including DNA information;
- for families or relatives:
  - administrative data (name, place of residence);
  - DNA information.

Sources include the missing individual (e.g., ante mortem or post mortem data), relatives, witnesses and other public or private bodies (government agencies, international and non-governmental organizations). The techniques and procedures used to search for the missing and identify human remains vary considerably depending on the context, time frame, scale of events and political situation. The extent and type of data collected may vary accordingly.

Activities following the collection of data can include:

- matching information from different sources, which may involve:
  - matching information collected from different private and public sources;
  - publicly disclosing collected information;
  - DNA analysis and matching;
- providing information on the results of the process to, for example:
  - living persons who are unaccounted for (when found);
  - families and relatives;
  - the public authorities;
  - private organizations.

The application of the principle of purpose specification entails limiting the collection and processing of data collected for purposes other than to establish the identity, whereabouts and fate of a missing person but which could be used for that purpose. Data collected for purposes other than identification may be processed only to the extent that they are used exclusively for the purpose of tracing and identifying missing persons (a vital interest of the missing person); furthermore, only the data needed or required for that purpose should be transferred by a third party holding such data (see *Principle 8* below). A third party holding personal data collected for another purpose is accountable for the use of the data that it transfers or discloses. In obtaining data on natural living or deceased persons from private or public sources, assurances should thus be sought that the data may be disclosed because:

- the data were collected to establish the identity, whereabouts or fate of missing persons;
- disclosure is not incompatible with the purpose for which the data were collected or obtained;
- the data are derived from publicly accessible sources (such as public or professional registers or published directories); or
- the disclosure serves a vital interest of the data subject or a close relative of the data subject and the data subject is physically or legally incapable of consenting to the disclosure.

Principle 5
Sensitive data should only be collected and processed with appropriate safeguards.

International and domestic texts lay down particular restrictions with regard to the processing of sensitive data. Safeguards are required to prevent unlawful discrimination and the use of personal information which would prejudice or be detrimental to the individual to whom it relates. Different safeguard mechanisms may be found in domestic legislation, either in general data protection legislation or in specific laws (e.g., protection of medical records, DNA profiles or criminal records). Under the Swiss *Data Protection Act*, the collection of sensitive data must be registered with the Swiss Federal Data Protection Commissioner. The French *Law on Personal Records* requires the express consent of the individual. The Argentine *Personal Data Protection Act* provides that no one may be obliged to provide sensitive personal data, which can only be collected "in circumstances of general interest authorized by law".

Sensitive data is defined in the UN Guidelines as data likely to give rise to unlawful or arbitrary discrimination. The Guidelines provide that such data should not be compiled. However, exceptions are permitted within the limits prescribed by international human rights instruments, i.e. those which define unlawful or arbitrary discrimination. Exceptions could also come within the general "humanitarian exception clause", which provides that "a derogation from these principles may be specifically provided for when the purpose of the file is the protection of the human rights and fundamental freedoms of the individual concerned or humanitarian assistance". It may therefore be permissible under the UN Guidelines to collect sensitive personal data for humanitarian reasons.

Article 6 of the CoE Convention states that appropriate safeguards should be adopted for sensitive data, but the Convention does not spell out what would constitute "appropriate safeguards". The CoM Recommendation regulating the use of personal data in the police sector states that “the collection of data on individuals solely on the basis that they have a particular racial origin, particular religious convictions, sexual behavior or political opinions or belong to particular movements or organizations which are not proscribed by law should be prohibited”. The collection of data concerning those factors may only be carried out if "absolutely necessary for the purpose of a particular inquiry" (2.4). EC Directive 95/46/EC similarly prohibits the processing of sensitive data, but provides for derogations, including where the "processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent".

In the context of the search for the missing and the identification of human remains, sensitive data such as ethnic origin, political or religious activities, memberships, etc., may be necessary to ascertain the whereabouts or the fate of missing

persons or the identity of human remains. Inasmuch as such collection is for humanitarian reasons or for the benefit of the person to whom the information relates, the collection and processing of sensitive data should be allowed. Special care should be taken, however, to ensure that the data is not used or disclosed in circumstances that would be detrimental to the individual concerned.

Principle 6
Personal data should be accurate, complete and updated as is necessary for the purpose for which they are used.

The extent to which the information should be accurate, complete and updated depends on its use. The information should be sufficiently accurate, complete and up-to-date to minimize the possibility that a decision detrimental to the individual is taken on the basis of inappropriate information.

This principle does not exclude the collection of incomplete or disputed information. Data that cannot be fully ascertained may be deemed to be accurate and up-to-date so long as the doubts or uncertainties about accuracy or up-to-dateness are recorded with the data. If such data are disclosed to third parties, they should be accompanied by the relevant qualifying statement or note.

Principle 7
Personal data should be protected by security safeguards appropriate to the sensitivity of the information.

Appropriate safeguards should be set in place to protect personal data against loss or theft, unauthorized access, disclosure, copying, use or modification, regardless of the format in which they are kept. The safeguards may involve both physical security (for example, restricting access to premises holding records) and technical security measures (for example, encryption and computer “fire walls”). Persons and staff handling or processing the data should be bound by an undertaking of confidentiality.

The nature of the safeguards will vary depending on the sensitivity of the information. More sensitive information should be safeguarded by a higher level of protection (see, for example, the Canadian Standards Association’s *Model Code for the Protection of Personal Information*).

c. Use, disclosure and transfer of personal data

Principle 8
Personal data may not be used, disclosed or transferred for purposes other than those for which they were collected without the consent of the person concerned, except if required by a substantial public interest or for the protection of the vital interests of the person concerned or of others.

The right to privacy requires that personal information be protected from disclosure. Personal information may only be disclosed for the purpose for which the information was obtained or compiled or for a use consistent with that purpose.

Domestic legislation can provide that, without authorization, personal information can only be used for the purpose for which it was obtained or for uses consistent with that purpose. However, in certain circumstances personal data may be used or disclosed without the individual's consent or knowledge. The personal data of third parties (next-of-kin, witnesses, other victims) may also have to be disclosed in order to search for a missing person. Exceptions are quite broad, and usually include specific circumstances:

- where disclosure is required for the purpose of law enforcement or to carry out an investigation or in judicial proceedings;
- where disclosure is required to prevent or lessen a serious or immediate threat to the health or safety of the individual or others;
- where disclosure would clearly benefit the individual to whom the information relates; or
- where the disclosure is for statistical or research purposes.

The German *Federal Data Protection Act* allows the use of data collected for another purpose if required by law, if the person to whom the data are related has consented, if it is evident that it would be in the interests of the person concerned and there is no reason to assume that he would withhold his consent if he knew of the other purpose, or if necessary to avert a grave infringement of another person's rights. Under the Canadian federal *Privacy Act*, personal information held by public authorities may be disclosed, *inter alia*, "if the public interest in disclosure clearly outweighs

any invasion of privacy that could result from the disclosure", or if "disclosure would clearly benefit the individual to whom the information relates".

Personal data should only be disclosed to third parties with the consent of the data subject for the purposes mentioned above in relation to the search and identification of missing persons. Where this is not obvious in the circumstances, or if consent may not be practically obtained, data should be provided on condition that they are only to be used for the purpose(s) for which they are provided. In certain circumstances, personal data collected for the purpose of establishing the identity, location and fate of missing persons may be provided to serve other interests of the person unaccounted for or his or her relatives, or a public interest, in particular in connection with criminal investigations or legal proceedings. The countervailing legitimate interests of the individual or of other persons must, however, also be considered (e.g., if there is a threat to the person's security).

Public disclosure of personal data (by making data available to the press or to the public) without the consent of the person to whom the information relates should be considered only if it manifestly serves to protect or ensure the vital interests of the person or another person and consent cannot be legally or practically obtained. The countervailing legitimate interests of the individual or of other persons against the publicity or publication must, however, also be considered.

The unlawful collection, processing or disclosure of personal data may give rise to civil liability if the person to whom the information relates suffers damages. In situations of armed conflict or widespread internal violence, respect for data protection principles is likely to be a low priority for those engaged in the conflict. The threat of civil liability for breaches of data protection rules would likely have little impact during the conflict. However, after the conflict, civil liability could be imposed for breaches. An aggrieved person could obtain some compensation where the improper collection, use or disclosure of personal information resulted in harm to the person.

Principle 9
Personal data may only be transferred to third parties respecting personal data protection principles.

The protection of personal data afforded by domestic legislation being geographically limited, a number of States have adopted rules on the export of personal information, subjecting such transmission to prior control, authorization or declaration. The Swiss law prohibits the transmission of personal data abroad if doing so represents a serious, albeit non-physical, threat to the persons concerned, in particular if the level of protection of personal information is not equivalent to that afforded by Swiss law. The transmission of sensitive data may be subject to more stringent conditions. The Swiss law provides that "no one has the right to transmit to third parties sensitive data or personality profiles without a justifiable cause". EC Directive 95/46/EC similarly restricts the transfer of personal data to third countries with an adequate level of protection.

The data controller should ensure, where possible and appropriate, that the other persons or bodies involved in collecting the data have acted and shall continue to act in accordance with any relevant and applicable data protection laws and regulations, to the extent that those laws and regulations are themselves compatible with international human rights, humanitarian and data protection laws and standards. The controller should also seek warranties that if it transfers personal information to a third party, the third party will abide by data protection principles, rules and regulations.

Principle 10
Personal data should be deleted as soon as the purpose of their collection has been fulfilled, or when no longer necessary. They may, however, be retained for a definite period if required for the benefit of the individual to whom they relate or if essential for the performance of the humanitarian tasks of the organization which collected the data.

Personal data should only be retained as long as is necessary for the fulfillment of the purpose specified for their collection. This principle is closely associated with the principle of purpose specification. Personal data no longer required to fulfill that purpose should be destroyed, erased or made anonymous. If personal data are to be used for a new purpose, the individual's consent should be sought.

In certain circumstances, personal data can be stored or retained. For instance, personal information that has been used to make a decision about the individual should be retained long enough to allow the individual access to the information after the decision has been made. Similarly, the information may be useful for the person to whom it relates in the course of civil or criminal proceedings. Data should not, however, be kept for an undefined period but deleted after the

predetermined period has lapsed. Given the mandate and activities of some humanitarian organizations, data files may nevertheless have to be kept for a long period after relations between the individual and the organization have been terminated. A longer retention period for humanitarian reasons may thus be allowed.

d. Access to personal information

Principle 11
Access to personal data should be granted to the individual to whom the data relate. Provision should also be made for the right to challenge the accuracy and completeness of the data and to have them amended as appropriate.

International texts and domestic legislation provide for a right of access to personal information for the person to whom the information relates. Appropriate procedures should be established for that purpose. The general principles on access found in the relevant international instruments and domestic legislation are the following:

- all persons have to be informed of the existence, use and disclosure of personal information relating to them;
- on request, a person has a right of access to that information and the right to obtain a copy;
- all persons have a right to challenge the accuracy and completeness of the personal information relating to them and to have it amended as appropriate, or at least to have a notation placed on their file indicating their desire to have the information corrected;
- remedies should be provided for in case those rights are denied.

However, in certain situations, an organization or a public authority may not be permitted by law to provide access to all the personal information it holds on an individual. In other cases, the organization or authority may have discretionary power to refuse to disclose data. Also, the personal data on individual files may consist not only of raw data, but also of subjective information such as opinions or instructions. Data may also come from sources other than the individual, including protected sources. And yet, the disclosure of such information could be detrimental to the individual or to other persons.

Restrictions of access to personal data are recognized in most international instruments. All domestic laws also provide for restrictions of the right of access to personal data. The Swiss *Personal Data Protection Ac*t provides that information can be withheld if the law so provides, or if the paramount interests of third parties so require. Federal bodies may also restrict access to personal data in the public interest or if access could imperil a criminal investigation. However, exceptions to the access requirement should be limited and specific and the reasons for denying access should be provided to the individual upon request. The Canadian *Privacy Act* provides as exceptions to the right of access personal information obtained in confidence, information relative to international affairs, defence, law enforcement and investigation, or information which could reasonably be expected to threaten the safety of individuals. Reasonable exceptions could thus include information which:

- contains references to other individuals or sources of information received in confidence;
- could reasonably be expected to be injurious to a public interest (national security, public order, etc.);
- could reasonably be expected to be seriously detrimental to the interests of other persons;
- could impede or jeopardize the purpose for which the information was collected.

If data related to a person making a request for access to his or her information can be separated from information related to other persons or other information that cannot be disclosed, it is not necessary to refuse access to all the information. However, if the information cannot be separated, the body holding the information may have a duty to balance the interests involved while considering the disclosure of the information, including balancing the interests of the person to whom the information relates against those of other persons if the information also relates to them, or public interests, as the case may be.

With regard to certain types of information, particular conditions may be applicable. Some acts of domestic legislation require that sensitive medical information be made available through a medical practitioner (for example, Switzerland) or that it not be disclosed where it would be contrary to the best interests of the individual (as in Canada).

The UN Guidelines provide for a right of access by the individual to whom the data relates only, but recognizes that exceptions may be made to allow a third party to access the data if such access is necessary to protect a public interest (national security, public order, etc.) or, *inter alia*, the rights and freedoms of others, provided that the exceptions are expressly specified in law.

Under the Argentine *Personal Data Protection Act*, the right of access to personal information may be exercised only by the person to whom the information relates, or his or her guardian. If the person to whom the information relates is dead, the right of access may be exercised by the heirs. The Swiss law does not provide for a right of access by any person other than the data subject concerned. However, federal bodies may transmit personal data to a third party if the data subject has given his consent or if, under the circumstances, such consent may be presumed. The Canadian *Privacy Act* provides that the head of a government institution may refuse to disclose any personal information about another individual, which would seem to indicate that information about another individual may be disclosed in certain circumstances. The basic rule is that personal information under the control of a governmental institution may not be disclosed without the consent of the individual to whom the information relates, except in specified circumstances. Exceptions include disclosure for the purpose for which the information was obtained or compiled, and for any purpose where, in the opinion of the head of the institution, disclosure would clearly benefit the individual to whom the information relates. Thus, unless disclosure of information to family members would be deemed to fall under the latter categories or unless consent is presumed, personal information would not be released to family members.

For humanitarian reasons -- to help locate missing persons and human remains -- it may therefore be necessary for data protection legislation in some States to be amended to allow access by third parties to such personal information for humanitarian reasons. Provisions in data protection legislation that allow disclosure "in the public interest" may be too vague to ensure that third parties seeking to locate missing persons can obtain access to the necessary information. These third parties could include family members or others with a legitimate interest in helping to locate the person. Alternatively, freedom of information legislation could be amended to allow certain persons a right of access to information about missing persons if that is in the interests of the missing person or family members, or if it would otherwise serve the public interest.

Another way to permit family members to have access would be to consider them to be agents of the missing person. They could therefore act in the place of the missing person, and obtain access to information about the person.

It should also be noted that the Argentine Supreme Court has held, in the context of access to information held by public authorities, that information relative to the fate of a family member (in the case at hand, a brother) who was the victim of a forced disappearance could be regarded as personal information, and thus subject to a right of access. A Brazilian high court, however, has taken the contrary view.

2.2 Identification of human remains: commonly accepted principles

Principle 1
The identity of human remains, and the cause of death, should be established by the competent public authority with due diligence.

In most domestic legislation, a death must be reported to a registrar or an *officier d'état civil* by the person responsible for registering the death, usually a relative of the deceased or, if there is no surviving family member, any other person able to identify the deceased. If the deceased cannot be identified, the death certificate must include a description of the body and an account of the circumstances surrounding its discovery. The body can be disposed of once the registrar has issued the appropriate certificate. Further requirements may be imposed in the case of cremation.

The purpose of certifying death is to confirm that death has occurred, to give an indication of the likely cause of death, to support interested persons if the cause of death is disputed, to ensure that deaths where criminal causes arise are investigated prior to the disposal of the body and to provide statistical information on causes of death. In most cases, the law requires that death be certified by a medical practitioner. In some cases, if death is obvious and cannot be certified by a physician within a reasonable time, it can be certified by a justice of the peace (e.g., *Civil Code* (Quebec (Can.), s. 123).

Before a death can be registered and the body disposed of, a medical certificate of cause of death must usually be provided by a doctor. Where the cause of death appears to be unnatural, sudden and unknown, or the result of violence, the death usually has to be reported to the authorities. As a rule, anyone who finds a body has the duty, as soon as is practicable, to report it to the police (e.g., *Coroners Act* (NZ), s. 5).

In most common law countries, suspicious deaths must be reported to a coroner or a medical examiner (e.g., *General Laws of Mass.* (US), chap. 38, sec. 3; *Coroners Act* (NZ), s. 4; *Act respecting the determination of the causes and circumstances of death* (Quebec (Can.)), ss. 34-36). This is usually done by the doctor certifying the death or by the police. The coroner is an independent judicial officer charged with a duty to investigate the circumstances of certain categories of death for the protection of the public. The coroner's inquest is a fact-finding exercise. It is not a trial and does not aim to establish criminal or civil liability. The coroner bears ultimate responsibility for identifying deceased

persons, and is also responsible for establishing the cause and time of death. Police responsibilities on behalf of the coroner include control of the remains, their identification and their release to the next-of-kin with the coroner's consent.

Under the UK *Coroners Act 1988*, "[w]here a coroner is informed that the body of a person (the deceased) is lying within his district and there is reasonable cause to suspect that the deceased (a) has died a violent or an unnatural death; (b) has died a sudden death of which the cause is unknown; (c) has died in prison or in such a place or in such circumstances as to require an inquest under any other Act, then the coroner shall as soon as practicable hold an inquest into the death of the deceased" (s. 8). The purpose of the coroner's inquest is to establish, as far is possible or as far as can be proved, that a person has died, the person's identity, when and where the person died, the cause of death, and the circumstances of death (e.g., *Coroners Act* (NZ), s. 15, *Coroners Act* (UK), s. 11). The Quebec Act requires the coroner to identify all unknown bodies, to confirm presumed identities and to establish the cause and manner of death. In other Canadian provinces, suspicious or unnatural deaths are investigated either by coroners or medical examiners. In the United States, investigations into deaths vary considerably from one jurisdiction to another. Some jurisdictions use the medical examiner system and others, the coroner system (the medical examiners are usually appointed, while coroners are elected). Medical examiners or coroners are responsible for investigating sudden and violent deaths. Deaths to be investigated vary from jurisdiction to jurisdiction, but usually include sudden, suspicious or unexplained deaths, including the identification of unknown corpses (e.g., *General Laws of Mass.* (US), chap. 38, sec. 2).

Section 74 of the French *Code of Penal Procedure* provides that:

> "When a body is discovered, if the cause of death is unknown or suspicious and irrespective of whether it is violent, the judicial police officer concerned shall immediately inform the public prosecutor, immediately visit the site of the discovery and make an initial report.
>
> The public prosecutor shall visit the site if he considers it necessary and shall require the assistance of persons able to appraise the nature of the circumstances of death. To that end, he may also delegate a judicial police officer of his choice [...]".

An investigation into the cause of death may also be mandatory under human rights instruments. Both the European and the American Courts of Human Rights have held that the protection afforded by the right to life entails determining the cause of death (see *McCann* v. *United Kingdom* (1996) 21 EHRR 97).

Principle 2
During an investigation or an inquest, including in the decision to perform a post mortem examination, the known religious beliefs and opinions of the deceased and his relatives should be taken into consideration.

In the case of a suspicious death, discovery of a corpse or where the death certificate mentions an obstacle to inhumation, most domestic laws provide that the body shall remain at the disposal of the judicial or investigating authorities for as long as necessary.

In French law, the body remains at the disposal of the judicial authorities and the death certificate is transmitted to the public prosecutor. Funeral operations are suspended until authorization is granted by the judicial authority, usually after a post mortem examination. It seems that, pursuant to a principle of public policy (*principe d'ordre public*), the search for the truth, i.e. the establishment of the cause of death, cannot be objected to. A post mortem examination can be ordered by the public prosecutor (*Procureur de la République*) or an investigating magistrate (*juge d'instruction*) in cases of violent or suspicious death (crime, suicide or accident).

In common law States, a post mortem examination may be performed where the coroner is to hold an inquest into a death or has opened but not completed an inquest, or to enable the coroner to decide whether to hold an inquest. The courts have recognized that the coroner has an absolute right of possession and control of the body from the time a report reaches the coroner that a person has been killed until the conclusion of the inquest. There is generally no statutory requirement to obtain consent from any natural or legal person before holding an inquest or directing a post mortem examination or special examination, and these may therefore be conducted notwithstanding lack of consent or even despite objections from relatives. The practice of coroners to retain the body for the purpose of post mortem examination has been endorsed by the courts.

In US law, tissue or other body parts may not be removed from a deceased person for forensic or scientific study without the consent of the person whose duty it is to bury the body (e.g., spouse or next-of-kin) unless authorized by statute. Such statutory authorization and the power to order an autopsy is generally granted to coroners, medical examiners or

attorneys-general for the investigation of suspicious deaths or the identification of human remains (e.g., *Mass. General Laws*, chap. 38, sec. 4).

In many Australian territories, unless the coroner believes that a post mortem must be performed immediately, the "senior next-of-kin" of the deceased person may object (e.g., *Coroners Act 1993* (NT) s. 23; *Coroners Act 1985* (Vic), s. 29). If the coroner believes that the post mortem is necessary, he must notify the senior next-of-kin and not perform the examination until 48 hours after the notification. This enables the next-of-kin to apply to the courts for an order preventing the post mortem. The Australian courts have held that cultural beliefs have to be taken into account, and that in certain circumstances the right of the next-of-kin to be spared further grief overrode the community's interest in discovering the actual cause of death (*Green* v. *Johnstone*, [1995] 2 VR 176 (Supreme Court of Victoria); *Re Death of Simon Unchango (Jnr), ex parte Simon Unchago (Snr),* (1997) 95 A. Crim. R. 65; in these cases involving the deaths of children, the deaths had not occurred in suspicious circumstances). An Australian Court of Appeal held that if a coroner was aware of the views of the family, he was required to take them into account.

Similar principles may be found in the New Zealand *Coroners Act*. The coroner, in deciding whether or not to authorize examination, has to have regard, *inter alia*,

- to the desirability of minimizing the distress caused to persons who, by reason of their ethnic origins, social attitudes or customs, or spiritual beliefs, customarily require bodies to be available to family members as soon as is possible after death;
- to the desirability of minimizing the causing of offence to persons who, by reason of their ethnic origins, social attitudes or customs, or spiritual beliefs, find the post mortem examination of bodies offensive;
- to the desire of any member of the immediate family of the person concerned that a post mortem examination should be performed (s. 8).

Under Quebec law, a post mortem examination carried out to establish the identity of the deceased or the cause of death does not require the relatives' consent. The *Coroners' Code of Ethics* nevertheless provides that the religious beliefs and opinions of the deceased and those of his relatives are to be respected to the extent that the requirements imposed by law so permit.

Principle 3
When determining the cause and circumstances of death, in particular during an investigation or an inquest, the dignity, honor, reputation and privacy of the deceased should be respected. All corpses in the custody and possession of an investigating authority should be treated with dignity and respect.

That the deceased should be treated in a decent and respectful manner consistent with the moral expectations of the community is recognized both in domestic legislation and by domestic courts. Most acts of domestic legislation provide that a body should not be subjected to any unnecessary or unauthorized procedure, treatment or exposure that is inconsistent with the wishes of the deceased or his family. This is also reflected in the codes of ethics of public officers and/or of physicians. The Quebec *Coroners' Code of Ethics* provides that the body shall be treated with dignity and respect. The French *Medical Code of Ethics* states that "the physician, whose duty is to the individual and to public health, shall perform his mission with respect for human life, the individual and his dignity. Respect for the person continues to be due even after death".

To improperly and indecently interfere with a dead body or human remains is a criminal offence under most domestic criminal legislation. Under the Canadian *Criminal Code* and the *Criminal Code* of Queensland (Australia), anyone who improperly or indecently interferes with or offers any indignity to a human body or human remains, whether buried or not, is liable to imprisonment. Under Article 262 of the Swiss *Penal Code*, "anyone who publicly insults or abuses a human body shall be liable to imprisonment or a fine". The French *Penal Code* provides that "any attack on the body's integrity, by whatever means, shall be punished by one year in prison or a fine of 15,000 Euros" (Art. 225-17).

Principle 4
Exhumations must be authorized by the competent authority.

In most countries, exhumation is subject to a range of rules relative to burial, ecclesiastical law and health protection.

As a rule, exhumations require authorization. In most States, they may be authorized by the local authorities or by order of a court for the purpose of a judicial enquiry. The Belgian law on funerals and burials provides, for instance, that "communal cemeteries (and crematoriums) are subject to the authorities, the police and the surveillance of the

communal authorities, which shall ensure that no act of disorder or disrespect for the memory of the dead is committed and that no body is exhumed without authorization". Under Malaysian law, exhumation may be authorized by order of a magistrate's court or under a licence granted by the local authorities (*Local Government Act*, 1976). The legislation governing coroners in common law countries usually provides that the coroner may order an exhumation where he reasonably believes that it may be useful for the performance of his duties.

In most national systems, exhumations may be carried out in the following circumstances: on the order of a court or a magistrate in civil cases (e.g., in parental filiation cases), in order to bury a body elsewhere or to repair the tomb, and on the order of a public officer whose duty it is to determine identity or the cause of death of a deceased person (e.g., *Civil Code* (Quebec (Can.), s. 49; *Coroners Act* (Victoria (Aust.), s. 30).

Principle 5
The decision to carry out an exhumation should take account of the interests of the next-of-kin.

It is usually the next-of-kin who request exhumation. The request is usually presented to the local civil or church authorities, depending on the place of burial. In Belgium and France, authorization for exhumation is granted by the local authorities. In the United Kingdom, a licence for exhumation is obtained from the Home Office, and a faculty from the Bishops Register if the remains are buried in consecrated grounds. Generally, the local official has some measure of discretion in granting the authorization. He must take into account the respect due to the dead and the maintenance of public order. Other family members may also oppose an exhumation. Disputes between the applicant and the local authority or between next-of-kin may be brought before civil or administrative courts, as the case may be.

The consent of next-of-kin is usually not required when the exhumation is ordered by an investigating officer, a magistrate or a judge. However, the Victoria, Western Australia and Tasmania Coroners Acts (Australia) provide that the coroner must notify the "senior next-of-kin" of the deceased and the trustees or owners of the cemetery, burial ground or place of burial before the body is exhumed unless it is not possible to do so. If the senior next-of-kin object to the exhumation, the body must not be exhumed until 48 hours after the request has been made. This allows the next-of-kin to apply for a court order prohibiting exhumation.

The presence of family members is not required under all domestic legislation. Only the presence of the public official or the magistrate who ordered the exhumation and a medical practitioner is generally required. When the exhumation is requested by a close relative, French law requires the presence of a relative or a family representative. In contrast, in the United Kingdom family members are usually not allowed to attend the exhumation.

Domestic legislation on exhumations is generally meant to be applied in ordinary circumstances. Particular methods and procedures may be more suitable in situations of armed conflict or internal violence, where the identity of the body to be exhumed is to be confirmed or where multiple or mass graves must be unearthed. Families, or the community, as the case may be, should be more closely implicated with the process of exhumation in such situations in order to facilitate acceptance of the process and its results.

Principle 6
Exhumations must be carried out in accordance with recognized standards, including health protection standards.

Most acts of domestic legislation require compliance with conditions outlined by the health authorities. Under Australian law, all exhumations are required to comply with the conditions set forth by health departments such as the Australian Capital Territory Department of Health and Community Care. Procedures for the protection of public health and for the protection of the persons carrying out the exhumation are provided for (e.g., protective clothing, use of disinfectant, etc.), and the exhumation must be carried out under the supervision of a public health officer. The presence of an Environmental Health Officer is required in the United Kingdom. Under Newfoundland (Canada) law, exhumations must be performed with the precautions prescribed by the Minister of Health (*Exhumation Act*, s. 2). The French *Code des communes* requires that a number of health precautions be taken.

Principle 7
Families should be kept informed of the decisions taken in relation to post mortem examinations, as well as of the results of any such examination.

Although there is no requirement to seek the consent of the relatives, certain people and agencies must be notified of the date and time of the proposed post mortem unless it is impracticable to do so or would cause the examination to be unduly delayed; this includes "any relative of the deceased who has notified the Coroner of his desire to attend, or be represented at, the post mortem examination" (Rule 7(2)(a)), 1984 Rules (UK)). The coroner has a discretionary power to notify any other person whom is not under a duty to notify. The *Practice Notes for Coroners*, issued by the UK Coroners' Society, advise that relatives and family of the deceased should be given appropriate information about a proposed post mortem.

Similarly, the Quebec *Coroners' Code of Ethics* stipulates that the coroner should provide the relatives of the deceased with information where the situation so requires. The UK Home Office Memorandum on good practice also provides that the victim's family should be kept aware of developments and given appropriate support. The next-of-kin should also be advised that the coroner's report is available. The UK *Model Coroner's Service Charter* provides that if a post mortem examination is necessary, the next-of-kin should be told why and what is involved, if they so request, be given advance notice of the arrangements, if practicable, and be sent a copy of the post mortem report at their request.

The New Zealand *Coroners Act 1988* provides that a coroner who has authorized a post mortem examination shall, as soon as is practicable after doing so, take all reasonable steps to ensure that a member of the immediate family of the person concerned receives notice that the performance of an examination has been authorized and of the coroner's reasons for authorizing it. Any member of the deceased's family can obtain a copy of the examination report from the coroner after seven days (s. 11).

The report on the post mortem examination is delivered to the coroner and may not be disclosed to any other person without his consent. The coroner must supply a copy of the report to any person who, in his opinion, is a "properly interested person" (on payment of a fee), but there is no statutory requirement for relatives to be provided with a copy of the post mortem report or notification of the result of the inquest. The *Practice Notes* provide, however, that "the relatives and family of the deceased person [...] should be told the result of the examination as soon as practicable, and in writing if they request it [...] It might be appropriate to offer to forward the result and a copy of the pathologist's report of the examination to their nominated medical attendant so that it can be explained to them".

In some situations, family members may not want to be informed of the circumstances of the death, since this might cause them unnecessary distress. That difficulty can be circumvented by forwarding the information to the family doctor, who can explain the circumstances of death, or by withholding information that members of the family might not wish to know.

Principle 8
The remains should be released to family members at the earliest time possible.

The accepted principle is that there is no property in a dead body. Indeed, it is a longstanding common-law rule that there is no property in a corpse (*Williams* v *Williams* (1880) 20 Ch. D. 659). The French *Civil Code* similarly recognizes that "the human body, its components and its products do not give rise to a right of ownership" (*Civil Code* (Fr.), Art. 16-1).

Once an inquest has been completed, the coroner or medical examiner no longer has the right to retain the body, which must be returned to its lawful possessors. English common law recognizes that a deceased's relatives have a possessory right in the body, corresponding to the duty to arrange for proper disposal. This duty falls primarily on the personal representative of the deceased. If no executor has been appointed, the first person entitled to deal with the estate of the deceased has the right of possession. The other persons who are charged by the law with the duty of interring the body include, for example, the parent of an infant child who dies, where the parent has the means to do so. As this right of possession is derived from the duty to dispose of the body, a body may be claimed only for that purpose.

In situations where body parts are scattered and not recovered at the same time, the family should be informed of that fact and asked whether it wants to be informed of the recovery of distinct remains once the identification has been definitively confirmed. To spare the families further grief, procedures for the identification of victims of the World Trade Center attack included giving families the option of leaving any identified remains at the morgue until testing was over (a single burial could then take place) or being notified only once the final confirmation had been made.

Delays in the release of remains when a post mortem examination is to be performed have been a concern for victims' families, in particular in criminal cases, where a second post mortem may be requested by the defendant. A UK Home Office circular on post mortem examinations and the early release of bodies contains a memorandum of good practice based on the following considerations:

- every effort is to be made for a decision on the need for a second post mortem to be taken as soon as possible;
- where no one is charged in connection with the death within a month, provision will be made for a second, independent, post mortem for use by a defendant in the future, if required;
- the body will be released for burial or cremation at the earliest opportunity;
- requests for multiple examinations by jointly charged defendants will be considered critically;
- all the individuals and agencies involved will seek to minimize delay, with the recommended time scales to be regarded as maxima.

The New Zealand *Coroners Act 1988* emphasizes the importance of releasing the body of the deceased as quickly as possible. It provides that as soon as the coroner is satisfied that it is no longer necessary to withhold the body from family members, he shall authorize its disposal forthwith (s. 14). The Act also permits the coroner to direct the doctor to perform a post mortem examination forthwith if relatives of the deceased have ethnic origins, social attitudes or customs, or spiritual beliefs which customarily require bodies to be available to family members as soon as is possible after death (s. 9).

Similarly, the Quebec *Coroners' Code of Ethics* provides that the release of the body shall be facilitated with all the diligence that the relatives of the deceased person may reasonably expect. The Quebec *Act respecting the determination of the causes and circumstances of death* provides that post mortem examinations are to be carried out with due diligence.

Principle 9
The body of the deceased should be restored before being returned to the next-of-kin. Families should be notified if body parts are retained.

A post mortem typically involves an examination of the exterior of the body. Small samples of tissue may be taken for analysis and body parts may be severed for the purpose of establishing the cause of death or identity. It would also seem to be normal procedure in coronial post mortem, in particular to establish the cause of death, to remove organs from the body; the heart and brain in particular may be retained and may not be available for burial or cremation with the rest of the body. Tissue blocks and slides are also generally made and retained. Coroners are usually not required to notify or obtain the consent of the deceased's family if body parts are to be removed and retained. Similarly the French *Public Health Code* provides that "there may be no removal for scientific purposes other than that carried out to establish the cause of death without the consent of the deceased expressed directly or via the family" (*Code de la santé publique* (Fr.), Art. L1232-3).

It has long been held by the courts of the United States that the right of relatives to the body of a deceased person "is the right to what remains when the breath leaves the body, and not merely to such a hacked, hewed, and mutilated corpse as some stranger, an offender against the criminal law, may choose to turn over to an afflicted relative" (*Burney* v. *Children's Hosp.* (1897)). Once the autopsy has been completed, the body parts that are not retained should be returned to the body, and the body reconstructed before being released. In South Australia, the funeral director is required to certify that the body has been delivered in an appropriate condition. The French *Public Health Code* states that "doctors who remove an item from the deceased's body are obliged to ensure the decent reconstruction of the body*" (Code de la santé publique* (Fr.), Art. L1232-5).

The common law is unclear as to whether each and every part of a body which might be discovered, for example after an accident, or after burial of the rest of the body, or every slide and tissue sample in a pathology laboratory following a post mortem examination, should be regarded as being within the definition of "the body'" for the purposes of the duty to dispose. Whether the right to call for possession of a body pursuant to the duty to dispose of it extends to parts of the body is thus uncertain. English and Australian courts have recognized in limited circumstances an exception to the common law rule that a dead body or part of such a body could not be property where the body or part has been altered by virtue of the application of skill. A recent decision in the Supreme Court of Western Australia held that a surgical tissue sample held by a pathology laboratory was property. At issue was whether the Court could make an order for a deceased's tissue sample to be used for DNA testing to establish whether the plaintiff was the natural daughter of the deceased (*Roche* v. *Douglas*). The extent of the skill which must be applied in order for a right to possession or property

in tissue to vest in the person applying the skill is, however, unclear. When there is a property right in the relevant body part, there is no longer any obligation to bury it. Thus, relatives would not have the right to claim possession for the purpose of burial.

Once authorization to perform a post mortem examination has been given, the domestic legislation of some countries authorizes the retention of body parts and tissues removed from the body for the purpose of the post mortem for transplantation or for therapeutic, medical or scientific purposes. Others do not.

Article 8 of the *European Convention of Human Rights* has been interpreted as protecting the individual against arbitrary interference by public authorities in his private or family life. The concept of "family life" has been construed broadly, although the question of whether the removal, retention and use of tissue from a deceased member of a family can be an interference with family life has not yet been determined.

2.3 Protection of genetic information: commonly accepted principles

Principle 1
The collection, use and disclosure of DNA profiles are subject to the rules relative to the protection of personal data.

DNA profiles contain personal information that is regulated by both international and domestic texts. Most national authorities responsible for the protection of personal data who have considered the subject of DNA data banks have maintained that the domestic legislation relative to the protection of personal information is applicable to the management, use and storage of DNA samples and profiles.

In some cases, specific provision had been made for this in national legislation. The Swiss draft law on the use of DNA profiles provides specifically that access to DNA information is subject to the provisions of the Federal Law on Data Protection, as is the transfer of DNA information abroad.

The management of the DNA data bank established at the federal level in Australia is the responsibility of an executive agency subject to the Australian *Privacy Act*.

Principle 2
Identification of human remains through DNA typing should only be undertaken when other investigative techniques of identification are not adequate.

A number of investigative techniques are used to identify human remains on the basis of skeletal features, dental records and fingerprints. Secondary evidence can be obtained from circumstantial items such as clothing and personal property. However, remains subjected to the violence of modern warfare or the ravages of time may no longer be suitable for the traditional means of identification. When biological remains cannot yield positive dental and fingerprint evidence, DNA typing may provide additional evidence in support of identification.

DNA profiling can only be used to confirm a person's identity when close blood relatives are available to give a sample against which samples from the body can be matched, unless ante mortem samples are available. In order to prevent distress to the relatives, DNA profiling should only be considered as a last resort when all other methods of identification have proved fruitless. This principle is recognized, for instance, in the Swiss draft law on the use of DNA profiles.

Principle 3
DNA samples may only be taken and analysed with the informed consent of the individual, except where an overriding public interest dictates otherwise.

That the consent of the individual is required is consistent with the principle of consent for the collection of personal data. It is also consistent with the protection of privacy as guaranteed under international human rights instruments.

Unless the samples are taken from suspects in the course of a criminal investigation or from convicted persons, the taking of samples and the analysis of DNA require the consent of the individual concerned under most domestic legislation. One exception to the general principle of consent outside a penal procedure is the obligation for members of the United States armed forces to provide DNA samples. This obligation to provide DNA samples has been challenged unsuccessfully before the courts.

The Explanatory Report to Council of Europe Recommendation R (92) 1 notes that there is a noticeable difference between the approaches of common law and continental countries with regard to the requirement of consent. In

continental countries, if consent is withheld, a court order may usually compel the taking of a sample in certain circumstances. In common law countries (e.g., the UK), if consent is withheld the taking of intimate samples may not be compelled; the refusal can, however, be held against the person who withheld consent. In practice, however, the may be no difference as there have been reports indicating that suspects or inmates were placed under pressure to consent to the taking of samples in many countries.

In the case of a missing person, consent is required from blood relations but not from the missing person (his/her representative or relatives). The Swiss draft law on the use of DNA profiles allows the analysis of biological material taken from someone who has disappeared in the event that the profile is needed for identification. The DNA profile of blood relations of missing persons may also be established, with their consent.

Few countries have domestic legislation providing precise guidelines on consent and on the information to be provided to the person voluntarily undertaking a forensic procedure. Most US legislation does provide, however, that the person undergoing a forensic procedure must be informed of the procedure (how the sample is to be taken) and that the information is to be stored in a DNA data bank. On the basis of the general rules on the collection of personal information, the following information should be provided to the person voluntarily undertaking a forensic procedure for consent to be informed:

- the way in which the forensic procedure is to be carried out;
- that the person is under no obligation to undergo the forensic procedure;
- that the person may at any time withdraw consent to undergoing the forensic procedure or for retention of the forensic material taken or of information obtained from the analysis of that material;
- that information obtained from an analysis of forensic material may be placed on a DNA database, and, if so;
- the purpose for which it is to be placed in that database and that the information may be used only for that purpose.

If consent is withdrawn, the forensic material taken should be destroyed and the information obtained from the analysis deleted as soon as possible.

Principle 4
Forensic procedures must be carried out by an appropriately qualified person.

Domestic legislation usually identifies the categories of persons authorized to carry out forensic procedures. The Australian *Model Forensic Procedures Bill* provides that blood samples are to be taken by a medical practitioner or a nurse, dental impressions by a medical practitioner or a dentist, and mouth swabs by a medical practitioner, a nurse, a dentist or a qualified person as prescribed by regulations (e.g., a police officer).

In certain cases, provision is also made for the involvement of the individual's medical practitioner or dentist in an intimate forensic procedure involving a suspect in a criminal investigation or a convicted person.

Principle 5
DNA information collected for the identification of missing persons or human remains may only be used and disclosed for that specific purpose.

In accordance with the principle of purpose specification, personal information may only be collected, used or disclosed for a specified purpose. The same principle should apply to the use of DNA profiles. Profiles analyzed for the purpose of identification should only be used for the purpose of identification (or in subsequent criminal investigations or civil suits, where the identity of the deceased is at issue). Other uses of information derived from DNA analysis – for example, attempting to determine the ethnicity of the person or his or her health status after the person has been identified or using DNA information for scientific research – should be prohibited.

In domestic law, this principle is implemented in two ways. In some countries (such as France and some states of the United States), DNA analysis is restricted to non-coding DNA, except to determine gender. This requirement was especially important for the French *Commission nationale de l'informatique et des libertés*. Another approach is to prohibit deriving from DNA analysis information other than that required for the purpose of identification. The draft Swiss law on the use of DNA profiles prohibits deriving (or disclosing) health information or other personal characteristics (except gender) from DNA analysis, unless it is necessary to so to identify someone.

The principle of purpose specification is also recognized in CoE Recommendation No. R (92) 1 on the use of analysis of DNA within the framework of the criminal justice system. The recommendation does not, however, restrict DNA analysis to the non-coding part of DNA. The experts thought that it "would unnecessarily restrict those countries which allowed for the use of coding DNA". The EU Council Resolution of 9 June 1997 on the exchange of DNA analysis results states in its preamble that "exchanging DNA analysis results for the purpose of investigating crimes should be restricted to exchanging data from the non-coding part of the DNA molecule".

Principle 6
DNA samples and profiles should be destroyed/deleted when the missing persons have been identified, unless they are required for related purposes.

Some domestic laws do not provide for the destruction of samples or the deletion of DNA information. Under Canadian law, if a person is convicted of an offence identified by the law, the information may be kept indefinitely unless the conviction is overturned. Generally, however, if the individual receives an absolute or conditional discharge (a less serious penalty than a conviction) or if the individual is a juvenile, access to the information is to be permanently removed and the samples destroyed after a defined retention period. UK legislation provides that the samples must be destroyed where the suspect is exonerated or the charges are withdrawn, but the DNA profiles can be kept. Other laws provide for a time period for the keeping of samples or information. Dutch law provides that data on people who are wrongly considered suspects must be removed, but other data may be kept for up to 30 years. Crime scene data is kept for 18 years.

In the case of mass DNA screens performed for the investigation of serious crimes, the practice seems to be to destroy the voluntary samples once the crime has been solved.

Principle 7
DNA analysis should only be performed by certified or accredited laboratories.

CoE Recommendation R (92) 1 lays down a number of criteria to be met by laboratories or institutions accredited to perform DNA analysis. They include:

- high professional knowledge and skill, coupled with appropriate quality control procedures;
- scientific integrity;
- adequate security of the installations and of the substances under investigation;
- adequate safeguards to ensure absolute confidentiality in respect of the identity of the person to whom the DNA analysis relates;
- guarantees that the conditions laid down by the Recommendation are followed.

It also recommends the establishment of procedures for the regular supervision of accredited laboratories.

Most domestic laws impose conditions on laboratories accredited to perform DNA analysis guaranteeing security and confidentiality. Procedures for regular supervision have been established under French law and in several American states (for example, New York and Massachusetts).

Principle 8
DNA samples, profiles and records should be adequately protected from unauthorized access and use.

Appropriate safeguards should protect DNA samples and information against loss or theft, unauthorized access, disclosure, copying, use or modification, regardless of the format in which they are kept. This protection may involve both physical security (for example, restricting access to premises holding records or samples) and technical security measures (for example, encryption and computer “fire walls”). Persons and staff handling or processing the data should be bound by a duty of confidentiality.

The draft Swiss law on the use of DNA profiles provides, for instance, that DNA profiles are to be kept separate from other personal information, and accessible only with a key number. Most other domestic laws do not have that specific requirement but require a level of security appropriate to the sensitivity of the information that DNA analysis may produce.

Principle 9

DNA profiles or samples should only be disclosed, transferred or compared in the context of international cooperation for the purpose of identification, and only with the consent of the persons concerned, except in determined cases. DNA samples should not be transferred except where the analysis is to be performed abroad.

Before sensitive data are transferred across borders, the authorities who transfer the data should specify what uses and disclosures are permitted to the recipient and receive valid assurances from the recipient that the information will be used and disclosed only for those purposes and that appropriate fair information principles will apply (for example, security measures, retention periods). Only then should the data be transferred.

Similar assurances should be taken if the transfer of DNA samples is required (e.g., for DNA analysis to be performed in a foreign laboratory). If DNA information is otherwise available, it is not appropriate to transfer DNA samples themselves, since this would increase the risk that additional tests might be performed on the DNA for purposes that the transferring country has not authorized.

3. Annexes

3.1 Overview of international texts on the protection of personal data

There is no binding specific global international instrument on the protection of personal data. Binding instruments have only been adopted at the European level.

A. General principles

The UN *Guidelines for the Regulation of Computerized Personal Data Files* (1990) were adopted by the General Assembly on the basis of reports submitted by Special Rapporteur L. Joinet of the UN Sub-Commission on Prevention of Discrimination and Protection of Minorities. The Guidelines, which are not binding, are meant to provide general orientations for national laws and regulations on personal data files in relation to the protection of privacy. Their scope of application extends to public and private computerized files (and with appropriate adjustment to manual files). They should also apply to governmental international organizations. The principles laid down in the Guidelines are similar to those laid down in the OECD Recommendation. They include: lawfulness and fairness in data collection, accuracy, purpose specification, interested-person access, non-discrimination, security and accountability. The Guidelines similarly provide that an authority should be responsible for supervising observance of the principles. This authority should offer guarantees of impartiality, independence vis-a-vis persons or agencies responsible for processing and establishing data, and technical competence.

On the regional level, in 1980 the OECD Council adopted the *Recommendation concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data*. The Guidelines include principles that should be taken into account in the domestic legislation of member States. They are the basis for most of the national laws adopted since. The Recommendation covers "any information relating to an identified individual or identifiable individual" and applies to data processing in the public and private sectors. The principles laid down by the Recommendation include: collection limitation (lawfulness and fairness), purpose specification, use limitation, security, openness, and individual participation. The Guidelines state that data controllers should be held accountable for compliance with the Guidelines.

On the European level, the protection of personal data is regulated by the Council of Europe *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (1981). The Convention was the first binding international instrument on data protection and has been ratified by 25 States. A further 8 States have signed but not ratified it, among them the Russian Federation, Poland and Turkey. Amendments allowing the European Communities to accede to the Convention were adopted in June 1999. An additional protocol to the Convention, adopted in November 2001, relates to supervisory authorities and transborder data flows, and requires the parties to establish independent supervisory authorities which ensure compliance with domestic laws.

The Convention applies to the private and public sectors. Contracting States may extend its scope of application to groups of persons (associations) or legal persons or to files not processed automatically. They can also exclude certain categories of files, if such categories are not regulated by domestic law. The principles laid down in the Convention are largely drawn from the OECD Principles. They include: lawfulness and fairness in data collection, purpose specification, accuracy, interested-person access, security and accountability.

The European Union *Directive on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data* was adopted in October 1995. The Directive applies to the processing of personal data by any person whose activities are governed by Community law, in the public and private sectors, but not to processing operations concerning public security, defence, State security, and State activities in the areas of criminal law. The principles laid down in the Directive are broader and more detailed than those contained in the UN Guidelines, the European Convention, or the OECD Guidelines. Although the Directive formally applies to matters governed by European law, domestic implementing legislation is likely to be wider in scope, in order to avoid the establishment of different legal regimes.

It does not seem that other regional groupings in America, Africa or Asia have adopted instruments or guidelines on the subject. The OAS Inter-American Juridical Committee has, however, started to study the question following a request from the OAS General Assembly, and a draft convention relative to the protection of personal information based on principles similar to the CoE Convention is being examined.

Both the right to privacy and freedom of information are protected under general human rights treaties. The European Court of Human Rights has rendered several decisions on the right to information in relation with the right to respect for one's private life. It has also considered that the storing and disclosure of personal information coupled with a refusal to allow the individual to whom the information relates to correct or refute the information amounted to an interference with

the right to respect for private life. The interference may be justified, however, if the conditions set forth in Article 8 (2) of the Convention are met (*Leander* case, 1987, § 48).

B. Principles applicable to specific categories of personal data

As a general rule, the principles laid down in the texts mentioned above are of general application. They are applicable to all types of personal data. There are, however, some adaptations, restrictions or exceptions with regard to certain categories of data.

All international instruments allow derogations from the general principles, if such derogation is provided for by law and is necessary for the protection of national security, public safety (*ordre public*), the person to whom the information relates, or the rights and freedoms of others.

Although subject to the general principles, some types of data or use of personal data are the subject of particular texts that clarify or specify the application of the general rules on particular issues. The Committee of Ministers of the Council of Europe has thus adopted a number of recommendations on data protection in specific fields. In the context of missing persons, the most relevant are Recommendation No. R (87) 15 regulating the use of personal data in the police sector (17 September 1987), Recommendation No. R (91) 10 on the communication to third parties of personal data held by public bodies, Recommendation No. R (92) 1 on the use of analysis of deoxyribonucleic acid (DNA) within the framework of the criminal justice system, and Recommendation No. R (97) 5 on the protection of medical data (13 February 1997).

Protection of data in the police sector

Recommendation 87(15) was adopted by the Committee of Ministers of the Council of Europe on 17 September 1987 as part of the Committee's sectoral approach to the adaptation of the data protection principles laid down in the Convention to the specific requirements of particular sectors. The recommendation, although not binding, is referred to in binding instruments, in particular the Schengen Agreement incorporated into the Treaty of Amsterdam and the Europol Treaty.

The general thrust of the Recommendation is that the collection and processing of personal data collected by the police are subject to the general framework of the Convention. However, the Convention itself makes it possible for the States parties to derogate from the basic principles laid down in the Convention in the interests of "the suppression of criminal offences" (Article 8 (2) of the European Convention on Human Rights also allows limitations on the right to respect for one's private life for the prevention of crime). The Recommendation aims to provide guidance on the interpretation of the derogation in the Convention when regulating the collection, use, etc., of personal data in the police sector.

The Recommendation is based on the following principles:

- the collection of personal data for police purposes should be limited to such as is necessary for the prevention of a real danger or the suppression of a specific criminal offence; any exception to this provision should be the subject of specific legal provision;
- where data concerning an individual have been collected without his knowledge, he should be informed that information is held about him as soon as the object of the police activities is no longer likely to be prejudiced;
- the collection of data on individuals solely on the basis that they have a particular racial origin, particular religious convictions, sexual behaviour or political opinions or belong to particular movements or organizations which are not proscribed by law should be prohibited, unless the collection of such data is absolutely necessary for the purposes of a particular inquiry;
- an independent supervisory authority outside the police sector should be responsible for ensuring respect for the principles of data protection.

Use of DNA analysis and information

CoE Recommendation No. R (92) 1 lays down a number of principles that should be taken into account in national legislation on DNA analysis for the purpose of identification of suspects or any other individual within the framework of the investigation and prosecution of criminal offences. They include:

- samples collected and DNA analysis and the information derived from such analysis for the purpose of the investigation and prosecution of criminal offences must not be used for other purposes;
- samples should only be taken in circumstances determined by domestic law;
- the taking of samples for DNA analysis should only be carried out with the consent of the person, but domestic law can admit that samples may be taken without the consent of the suspect in determined circumstances;

- the collection of samples and the use of data analysis must be in conformity with the standards of protection of personal data;
- samples and body tissues should not be kept after the rendering of the final decision in the case in which they were used, unless it is necessary for purposes connected to those for which they were used; DNA analysis and the information so derived should be deleted when it is no longer necessary to keep it for the purposes for which it was used. Exceptions include:
  - where the individual concerned has been convicted of serious offences against the life, integrity and security of persons;
  - when the person so requests;
  - when the sample cannot be attributed to an individual (crime scene samples);
  - when the security of the State is involved;
- a procedure for the control and accreditation of laboratories performing DNA analysis should be established.

3.2 Overview of a number of domestic texts on the protection of personal data

Prompted by the OECD Guidelines and the European Convention, a number of States have adopted, or revised, their laws on the protection of personal data. The laws of only a few States are referred to here, namely Argentina, Canada, China (Hong Kong), Russia, Switzerland and the United Kingdom.

A. Argentina

Article 43 of the Argentine Constitution, enacted in 1994, provides a right of access to personal data held by public or private bodies. It states that "*Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquellos. No podrá afectarse el secreto de las fuentes de información periodística.* [Every person may file an action to obtain knowledge of the data about them and its purpose, whether contained in public or private registries or databases intended to provide information; and in the case of false data or discrimination, to suppress, rectify, make confidential, or update the data. The privacy of news information sources may not be affected.]" (Translation from Privacy & Human Rights, 2001) Such right is also included in the constitutions of several Argentine provinces. In 1999, the Supreme Court of Argentina, ruling in the *Urteaga* case, allowed an individual access to personal information held by the authorities about his brother who had disappeared during the military government. It held that information on the whereabouts of the claimant's brother should be regarded as personal information relative to the claimant.

Ley 25.326 de protección de los datos personales (the Personal Data Protection Act) was adopted in October 2000. It is based on seven basic principles, which are more or less common to international and domestic texts on the subject:

- the personal data collected must be accurate, adequate, relevant and not excessive in regard to the purpose for which they were collected;
- personal data may not be collected using unfair, fraudulent or unlawful means or methods;
- personal data may not be used for purposes different from or incompatible with those for which they were collected;
- the data must be exact and updated, as necessary; inaccurate or incomplete data must be deleted, replaced or completed, as the case may be;
- data must be stored in such a way as to permit the exercise of the right of access by the data subject;
- data which is no longer necessary for or relevant to the purpose for which it was collected should not be kept;
- the individual's free and informed consent is required for the collection, process and use of personal data.

B. Canada

There is no explicit right to privacy in Canada's Constitution and Charter of Rights and Freedoms. However, in interpreting Section 8 of the Charter, which grants the right to be secure against unreasonable search or seizure, the Canadian courts have recognized an individual's right to a reasonable expectation of privacy.

Privacy legislation covering government bodies exists in almost all provinces and territories. In some provinces, the law also regulates the collection and use of personal information held by the private sector. Nearly every province has some

sort of oversight body, but their powers vary. The federal *Privacy Act* regulates the protection of personal information under the control of federal governmental institutions. The Act contains provisions relative to the confidentiality, collection, correction, disclosure, retention and use of personal information by federal bodies. Individuals may request records of personal information directly from the institution that has custody of the information. The Act also establishes the Office of the Privacy Commissioner. Access to federal government-held information, including personal information, is regulated by the *Access to Information Act*.

The *Personal Information Protection and Electronic Documents Act 2000* governs the collection, use and disclosure of personal information collected and used by federal undertakings or businesses operating under federal jurisdiction (e.g., transport or communication enterprises). Part 1 of the Act establishes a right to the protection of personal information collected, used or disclosed in the course of commercial activities. Schedule 1 to the Act is the Model Code for the Protection of Personal Information, which was developed by a Canadian Standards Association (CSA) committee comprising consumer, business, government and labour representatives. The Code includes the following principles:

- an organization is responsible for the personal information under its control;
- the purpose of the collection of information must be identified;
- the knowledge and consent of the individual are required;
- the collection of information should be limited to that which is necessary for the purposes identified;
- personal information shall not be used or disclosed for other purposes;
- personal information shall be accurate, complete and updated as necessary;
- personal information shall be protected by appropriate security safeguards;
- access to the information collected shall be granted to interested persons;
- an individual shall be able to challenge compliance with the principles of protection of personal data.

C. China (Hong Kong)

The *Personal Data (Privacy) Ordinance* was enacted in 1995 and took effect in December 1996. The Ordinance was drafted on the basis of recommendations made by the Hong Kong Law Reform Commission. Data protection principles drawn from various domestic laws and from the EU Directive are also reflected in several provisions. A schedule to the Ordinance lays down data protection principles, including purpose specification, consent, accuracy, security and access.

The Ordinance applies equally to the public and private sectors. It lays down additional restrictions on certain types of processing, namely data matching, transborder data transfers and direct marketing. The transfer of data to foreign jurisdictions is subject to restrictions similar to those laid down in the EU Directive. The Ordinance establishes the Office of the Privacy Commissioner to promote and enforce compliance with statutory requirements.

A *Code on Access to Information* requires civil servants to provide records held by government departments unless the information requested falls into specific categories, including defence, external affairs, law enforcement and personal privacy.

D. Russian Federation

The Constitution of the Russian Federation recognizes rights of privacy. Article 24 of the Constitution further states that "it shall be forbidden to gather, store, use and disseminate information on the private life of any person without his/her consent". Access to any documents and materials directly affecting individual rights and liberties is also guaranteed unless otherwise stipulated under the law.

The *Law of the Russian Federation on Information, Informatization and Information Protection* was adopted in January 1995. It covers both the public and private sectors. A code of fair information practices on the processing of personal information is also provided for. It prohibits the use of personal information to "inflict economic or moral damage on citizens". The use of sensitive information is prohibited. Citizens and organizations have the right of access to information on them, and the right to correct and supplement it.

The Russian law does not establish a central regulatory body for data protection and it is not clear that it has been effective. The law specifies that responsibility for data protection rests with the data controllers. The law is overseen by the Committee of the State Duma on Information and Informatization and the State Committee on Information and Informatization under the Russian President’s authority. The law is presently being reviewed to bring it into line with the CoE Convention and the EU Directive.

E. Switzerland

Article 13 of the Swiss Constitution states that: "*toute personne a le droit d'être protégée contre l'emploi abusif des données qui la concernent*" (all persons have the right to be protected against misuse of their personal data).

The Federal Data Protection Act of 1992 (*Loi fédérale sur la protection des données*) regulates the protection of personal information processed by federal governmental bodies and by private persons. There are also separate data protection acts for the *cantons*. The federal Act requires that information must be legally and fairly collected and places limits on its use and disclosure to third parties. Federal agencies must register their databases and private companies must register if they regularly process sensitive data or transfer the data to third parties. Individuals have a right of access to correct inaccurate information. There are criminal penalties for violations. Transfers to other countries must be registered and are permitted only if personal data is protected in the recipient country as under Swiss law (in July 2000, the European Commission determined that Swiss law was adequate under the EU Directive).

The federal Act does not apply to personal data processed by the ICRC.

F. United Kingdom

The United Kingdom does not have a written constitution. The *Human Rights Act* (1998) incorporated the European Convention on Human Rights into domestic law, thus establishing an enforceable right of privacy.

The *Data Protection Act 1998* was adopted in July 1998 and came into effect on 1 March 2000. The Act was approved to make the 1984 *Data Protection Act* consistent with EU Directive 95/46/EC. It provides for limitations on the use of personal information and access to data and requires that entities that maintain records register with the Data Protection Commissioner. It covers data held by government agencies and private entities. The Act applies to personal data on living individuals only.

3.3 Overview of domestic laws and regulations on DNA analysis

A. Argentina

The Argentine law of 1986 on the establishment of a DNA bank was adopted to collect genetic data to assist in the resolution of disputes relative to parental filiation. The database was especially established to deal with the problem of the disappeared children of persons held in detention during the military dictatorship. The database (*Banco nacional de datos genéticos* (BNDG)) is run by a single institution, Durand Immunology Hospital of Buenos Aires, which is under the authority of the municipality of Buenos Aires. Its purposes are to organize and administer DNA data archives and to perform such studies or genetic expertise as requested by the judicial authorities.

The law applies to the identification of persons both in the course of legal proceedings involving issues of parental filiation and outside formal legal proceedings. The BNDG centralizes the information and analyses relative to children who have been or are to be identified in order to determine their filiation, as well as those of the members of their presumed families.

In the course of a legal procedure, when it is necessary to establish filiation in a claim that appears credible or reasonable, genetic tests may be ordered by the court. The assessment of the genetic evidence is made by the judge, taking into account the scientific knowledge in the field. No party is obliged to submit to a genetic test, however, failure to do so will be held against him, i.e. it will constitute an element of evidence against his claim. Outside formal court procedures, any blood relative of a child who disappeared or was presumably born in detention has the right to request and obtain the services of the BNDG.

B. Australia

In Australia, a number of laws at the state and federal level contain forensic procedure provisions affecting the collection, storage, analysis and disclosure of genetic information. The Model Criminal Code Officers Committee of the Standing Committee of Attorneys-General published the *Model Forensic Procedures Bill* to act as a guide for the territories in developing or enhancing their DNA legislation.

At the federal level, the *Crimes Amendment (Forensic Procedures) Act 1997* introduced provisions from the Model Criminal Code into the federal *Crime Act 1914*. It incorporated recommendations made by a consultative committee on police powers of investigation as well. The Act lays down the legal regime for the performance of forensic procedures during the investigation of Commonwealth offences and for the storage, use and destruction of material derived from these procedures. The *Crimes Act* was further amended in 2001 to expand the scope of coverage and provide for the establishment of a DNA database system.

The *Crimes Amendment (Forensic Procedures) Act 2001* applies to forensic procedures on suspects, persons convicted of a serious offence and volunteers. The definition of "forensic procedure" does not include "the taking of any sample for the sole purpose of establishing the identity of the person from whom the sample is taken". A "volunteer" means a person who volunteers to a police officer to undergo a forensic procedure, or, in the case of a child or incapable person, whose parent or guardian volunteers on the child or incapable person's behalf to a police officer that the child or incapable person undergo a forensic procedure.

A forensic procedure may be carried out with the informed consent of the suspect, or if a suspect or convicted person withholds consent, the procedure may be ordered by a senior constable or by a magistrate, depending on the case. Non-intimate procedures may be carried out without the suspect's consent on the order of a senior constable. An order from a magistrate authorizing the carrying out of the procedure must be obtained before an intimate procedure can be carried out on a suspect who has not consented. To give informed consent, the suspect must know how the forensic procedure is to be carried out, the purpose for which the forensic procedure is required, that consent may be withheld, and the consequences of withholding consent. The consequences of not consenting differ, depending on whether the forensic procedure is non-intimate or intimate and whether the suspect is in custody or not. For volunteers, informed consent includes the way in which the forensic procedure is to be carried out, that the volunteer is under no obligation to undergo the forensic procedure, that the volunteer may at any time withdraw consent to the forensic procedure or to retention of the forensic material taken or of information obtained from the analysis of that material, that information obtained from analysis of forensic material may be placed on the DNA database system, the purpose for which it is to be placed on that index and that the information may be used only for that purpose, and that information placed on the DNA database system will be retained for such period as the volunteer agrees and must then be removed from the system.

C. Canada

The Canadian Parliament adopted the *DNA Identification Act* in 1998. The Act provides for the establishment of a national DNA data bank and regulates the use of collected information and its transmission. If a person is convicted of a listed offence, the information may be kept indefinitely unless the conviction is overturned, if the individual is conditionally discharged of a conviction or if the individual is a juvenile and the specified retention period has expired.

The Act allows a judge to order the taking of samples from people convicted of a range of offences, including even common assault.

D. France

The French Civil Code states that the identification of persons by DNA analysis may only be carried out in the framework of judicial investigative proceedings, or for medical or research purposes. In civil matters, DNA analysis can only be used in cases where parental filiation has to be established. The first national permanent database of DNA profiles was established in 1998. Only the DNA profiles of persons convicted of serious crimes and crime scene traces are included in the database. Access to the national database is restricted to personnel from a specific unit of the Ministry of Interior and the *Gendarmerie*.

The taking of DNA samples is subject to the general principle of the inviolability of the human body laid down in Article 16-1 of the French Civil Code. The taking of an intimate sample is prohibited without the consent of the individual in all circumstances. Whether consent was a prerequisite in criminal proceedings was debated when the law incorporating Article 16-1 into the Civil Code was adopted in 1994. Given that the law is silent on the matter (an amendment for that purpose was not adopted), a majority of commentators are of the opinion that consent for the taking of intimate samples is required in all cases. However, persons convicted of crimes who withhold consent are liable to imprisonment and fine.

The legal requirements for taking and analysing DNA samples are not similar in civil and in criminal matters. In civil matters, a rule of "double consent" is applicable, i.e. consent must be obtained both to take the sample and to analyse the DNA. In criminal investigations and proceedings, consent is only required for the taking of intimate samples. It is not required for their analysis.

The laboratories that perform DNA analysis are accredited by a committee of the Ministry of Justice (*Garde des Sceaux*) and chaired by a magistrate of the Court of Cassation. Accreditation is granted for five years and is renewable. Quality control of laboratories is monitored by a public authority (*Agence du médicament*) in order to ensure, *inter alia*, the reliability of identification made by biological analyses using DNA profiles. Conditions of accreditation include the installations and equipment needed to ensure the absence of contamination, as well as the security and confidentiality of samples and results of analyses.

The law provides that only the non-coding part of the DNA molecule may be analysed (except to determine sex). DNA profiles are kept in the national database for 40 years.

E. New Zealand

The *Criminal Investigations (Blood Samples) Act* was adopted in 1995 and entered into force in 1996. Under the Act, DNA samples from persons convicted of certain offences, volunteers and suspects are entered in a national data bank.

While the Act was still under consideration, New Zealand's Privacy Commissioner expressed concern over some of the legislation's provisions. While noting the presence of certain safeguards, the Commissioner objected to the inclusion of voluntary samples from innocent people. He stated in a report regarding the proposed legislation that only samples from those convicted of serious offences should be entered into the data bank.

F. Switzerland

The Swiss *Projet de loi fédérale sur l'utilisation de profil ADN dans la cadre d'une procédure pénale et sur l'identification des personnes inconnues ou disparues* of November 2000 has not yet been discussed in parliamentary commission in the federal chambers. The law should enter into force before the end of 2004, when the current transitory regime will be terminated (*Ordonnance* of 31 May 2000). The main principles of the draft law are the following:

- the management of DNA samples and profiles is subject to the principles and rules relative to the protection of privacy and personal data;
- only certain public authorities (police, investigating magistrate, penal judge, or other persons competent for the identification of unknown persons) may order the taking of samples and their analysis;
- it is prohibited to try to extract health information from DNA analysis, to store or to transmit such data to a third party if the analysis should reveal such information;
- samples, analyses and profiles may only be used for the purposes laid down in the Act, i.e. penal proceedings or identification of unknown or disappeared persons;
- no samples may be taken without consent; if consent is withheld, the taking may be ordered by a judicial authority in the case of penal proceedings;
- for the identification of unknown or disappeared persons, DNA analysis may only be resorted to if there are no other practical means to proceed with the identification, or if the person cannot identify himself;
- in the context of the identification of unknown or disappeared persons, the sample must be destroyed and the profile deleted when the identification had been completed, or where it is no longer of any use;
- only accredited laboratories may perform DNA analysis;
- DNA profiles and other personal information are stored in different databases to avoid unauthorized disclosure of information.

G. United Kingdom

The *UK Police and Criminal Evidence Act 1984* already provided for comprehensive forensic procedures. The *Criminal Justice and Public Order Act 1994* extended the circumstances in which body samples may be taken and made possible the operation of a national DNA database.

The Act allows the sampling and storing of DNA from any individual who has been convicted, cautioned or is suspected of committing a recordable offence. Non-intimate samples can be taken without consent from a person in police detention if authorized by an officer of at least the rank of an inspector who has reasonable grounds for suspecting the involvement of that person in a recordable offence; a person charged with, or who has been informed that he will be reported for a recordable offence; or any person convicted of a recordable offence. Intimate samples may be taken from any person in police detention if authorized by an officer of at least the rank of an inspector, and if consent is given. Consent is required but adverse inferences may be drawn by a court if consent is withheld. The 1994 Act reclassified mouth swabs as "non-intimate", thus allowing the taking of such samples without consent.

The British system authorizes law enforcement agencies to take samples from people arrested for crimes before conviction. If the person is acquitted, the sample is expunged. If a match is found in the interim, it can be used by law enforcement agencies even if the person is later acquitted of the crime for which he was originally arrested. The samples must be destroyed where the suspect is exonerated or charges are withdrawn; the DNA data can be kept.

Mass DNA screens are performed for the investigation of serious crimes. During a particular investigation, voluntary samples are requested from a group of people, usually from a geographic region. The samples are put into a separate database for comparison with samples from a specific crime scene. Once the crime is solved the voluntary samples are

destroyed, and they are always kept separate from the main database. DNA profiles obtained voluntarily in the course of the investigation of a specific offence cannot be used in connection with the investigation of another offence.

H. United States

Starting with Colorado in 1988, all fifty states have now enacted statutes creating a DNA database. Legislation differs greatly from state to state as to the types of offenders included in the databases and also as to the allowed uses of the databases themselves. Most states allow the databases to be used for criminal investigations of any kind. Some states, however, restrict the types of criminal investigations allowed, while others also allow the use of the data in civil cases upon court order. Most state legislation has the following features:

- only authorized qualified persons may take samples;
- the person whose sample is collected has a right of access to the information and the right to know it is included in the database;
- the person has the right to request the deletion of the record if the conviction is overturned;
- unauthorized disclosure of the information and tampering with samples are subject to criminal penalties.

The constitutionality of some state legislation has been challenged before the courts on the basis, *inter alia*, of the IVth Amendment to the US Constitution protecting people against unreasonable search and seizure. In one of the most recent cases, the plaintiffs challenged the validity of a Massachusetts DNA database statute, which requires involuntary collection of blood samples from all persons convicted of one of 33 different types of offences. It was argued that the statute allowed for an unconstitutional search and seizure under both the federal and state constitutions. The Massachusetts Superior Court agreed and issued a preliminary injunction against the statute. The decision was reversed by the Massachusetts Supreme Judicial Court, which agreed that the taking of a DNA sample constitutes a search and seizure, but held that it was not unreasonable. It considered that a prisoner's reasonable expectation of privacy in his identity is diminished, and that there is a strong governmental interest in a "particularly reliable form of identification". After weighing the strong state interest and the reduced expectation of privacy against the level of intrusiveness of the test, it considered that constitutional requirements were met. In another case involving the Connecticut statute establishing a DNA data bank, the Second Circuit of the United States Court of Appeals reached a similar conclusion, albeit on other grounds.

In addition to the states DNA databases, the FBI has created a national DNA database. The *DNA Identification Act 1994 Act* allows the FBI to establish an index of DNA identification records of persons convicted of crimes and analyses of DNA samples recovered from crime scenes and from unidentified human remains. A 1999 amendment provided for the addition of analyses of DNA samples from relatives of missing persons. CODIS includes only DNA identification records and DNA analyses made by or on behalf of a criminal justice or law enforcement agency. It includes DNA identification records and DNA analyses maintained by federal, state and local criminal justice agencies pursuant to rules that allow disclosure of stored DNA samples and DNA analyses only:

- to criminal justice agencies for law enforcement identification purposes;
- in judicial proceedings, if otherwise admissible pursuant to applicable statutes or rules;
- for criminal defence purposes, to a defendant, who shall have access to samples and analyses performed in connection with the case in which such defendant is charged; or
- if personally identifiable information is removed, for a population statistics database, for identification research and protocol development purposes, or for quality control purposes.

Massachusetts

The given legislative purpose of the statute establishing the DNA data bank is to "assist local, state and federal criminal justice and law enforcement agencies in: (1) deterring and discovering crimes and recidivistic criminal activity; (2) identifying individuals for, and excluding individuals from, criminal investigation or prosecution; and (3) search[ing] for missing persons". Any person convicted of the perpetration of any of 33 enumerated crimes must submit a DNA sample to the State crime laboratory.

Two sets of emergency regulations have been promulgated concerning the collection, submission, receipt, identification, storage and disposal of DNA samples and the testing and analysis, quality assurance, computerized storage, retrieval and dissemination of the DNA database. The first set of regulations contains provisions that identify those individuals who may collect DNA samples, details the materials and procedures that those individuals must use to collect the samples and ensure that they are not contaminated, and establishes identification and record-keeping procedures the

collectors must utilize during the collection process. In addition, the regulations set forth procedures to be used by evidence technicians, to receive the samples and record the details necessary for proper identification. The regulations also specify handling and storage procedures for the DNA samples and their accompanying collection and information cards. All samples and collected information are to be "stored indefinitely in a secure storage area".

The second set of regulations spells out the methods to be used to analyse DNA samples, and security measures to prevent unauthorized access to, or disclosure of, information in the DNA database. The regulations specify that the DNA database "shall be comprised of data generated from STR testing" (STR testing involves only the non-coding part of DNA). The regulations go on to outline procedures the director must use to authorize access to the database, and limit more strictly the reasons for which DNA samples and analyses may be disclosed. These regulations also contain provisions describing the procedure for the deletion of records.

Failure to furnish a DNA sample required by the statute is liable to penal sanction or fine. If a conviction is subsequently overturned and then dismissed, relevant DNA records may be expunged by court order upon request by the person whose DNA record has been included in the database.

The Act limits access to, and use of, the information obtained from DNA samples. DNA records are confidential, are not included in the criminal offender record information system, and may be disclosed only as authorized by the Act. They can be disclosed only:

- to criminal justice agencies for law enforcement identification purposes;
- for criminal defence purposes, to a defendant, who has access to samples and analyses performed in connection with the case in which he is charged;
- at the discretion of the director of the crime laboratory within the state police department, to assist in the identification of human remains from mass disasters or to identify whether such remains are from those of a missing person, or to advance other humanitarian causes.
- if personally identifiable information is removed, for a population statistics database.

New York

The New York State DNA identification index was established in 1994. It contains the DNA profiles of persons convicted of specified felonies (among others, murder, rape, assault, attempted murder, sodomy, witness intimidation or criminal use of a firearm).

It is not expressly provided that only the non-coding part of DNA shall be analysed. However, it is provided that laboratories shall perform DNA analysis only for those "markers having value for law enforcement identification purposes".

The law does not provide for a time period for the expunging of records. However, upon notice of a reversal of conviction or the granting of a pardon to a person whose DNA record has been stored, the record is to be expunged from the database. Samples and sample analyses in possession of any law enforcement agency or any forensic laboratory are to be returned to the individual.

All records, findings, reports and results of DNA testing performed on any person are confidential and may not be disclosed without the consent of the subject of such DNA testing, except in a criminal proceeding to the court, the prosecution and the defence. Records maintained in the DNA database may only be disclosed:

- to a federal law enforcement agency, or to a state or local law enforcement agency or district attorney's office for law enforcement identification purposes or to assist in the recovery or identification of specified human remains, including identification of missing persons;
- for criminal defence purposes, to a defendant or his or her representative, who shall also have access to samples and analyses performed in connection with the case in which such defendant is charged;
- after personally identifiable information has been removed by the division, to an entity authorized by the division for the purpose of creating or maintaining a population statistics database or for identification research and protocol development for forensic DNA analysis or quality control purposes.

The unlawful disclosure of DNA records or of the results of a forensic DNA test or analysis is subject to penal sanctions.

3.4 International and domestic texts cited

A. International texts

Guidelines for the Regulation of Computerized Personal Data Files, General Assembly resolution 45/95 of 14 December 1990.
<http://www.unhchr.ch/html/menu3/b/71.htm>

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28 January 1981.
<http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm>

Recommendation No. R (87) 15 regulating the Use of Personal Data in the Police Sector, Committee of Ministers, Council of Europe, 17 September 1987.
<http://www.legal.coe.int/dataprotection/Default.asp?fd=rec&fn=R(87)15E.htm>

Recommendation No. R (91) 10 on the Communication to Third Parties of Personal Data Held by Public Bodies, Committee of Ministers, Council of Europe, 9 September 1991.
<http://cm.coe.int/ta/rec/1991/91r10.htm>

Recommendation No. R (92) 1 on the Use of Analysis of Deoxyribonucleic Acid (DNA) within the Framework of the Criminal Justice System, Committee of Ministers, Council of Europe, 10 February 1992.
<http://cm.coe.int/ta/rec/1992/92r1.htm>

Recommendation No. R (97) 5 on the Protection of Medical Data, Committee of Ministers, Council of Europe, 13 February 1997.
<http://cm.coe.int/ta/rec/1997/97r5.html>

Recommendation concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data, OECD Council, 23 September 1980.
<http://www1.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM>

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data, Official Journal L 281 , 23/11/1995 p. 31.
<europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html>

B. Domestic laws

a. Protection of personal data

Argentina

Ley 25326 - Protección de los datos personales, 4 October 2000, Boletín Oficial, 2 November 2000.
<www.jus.gov.ar/minjus/oac/ley25326.pdf>.

Australia

Privacy Act 1988, Act No. 119 of 1988.
<http://www.austlii.edu.au/au/legis/cth/consol_act/pa1988108.txt>

Belgium

Loi relative à la protection des données à caractère personnel, 8 December 1992.
<http://www.privacy.fgov.be/textes_normatifs/version_coordonnée.pdf>

Canada

Access to Information Act, R.S. 1985, c. A-1.
<http://laws.justice.gc.ca/en/A-1/text.html>

Privacy Act, R.S. 1985, c. P-21.
<http://laws.justice.gc.ca/en/P-21/text.html>

Personal Information Protection and Electronic Documents Act, 2000, c. 5.
<http://laws.justice.gc.ca/en/P-8.6/text.html>

Chile

Ley 19628 - Protección de datos de carácter personal, 18 August 1999.

China (Hong Kong)

Personal Data (Privacy) Ordinance, Ord. No. 81 of 1995.
<http://www.privacy.com.hk/contents.html>

France

Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, Journal officiel, 7 January 1978.
<http://www.cnil.fr/textes/text02.htm>

Germany

Federal Data Protection Act (translation), 20 December 1990, BGBl.I 1990 S.2954.
<http://www.datenschutz-berlin.de/gesetze/bdsg/bdsgeng.htm>.

Russian Federation

Law on Information, Informatisation and Information Protection (translation), 25 January 1995.
<http://www.datenschutz-berlin.de/gesetze/internat/fen.htm>

Switzerland

Loi fédérale sur la protection des données, 19 June 1992.
<http://www.admin.ch/ch/f/rs/235_1/>

Ordonnance relative à la loi fédérale sur la protection des données, 14 June 1993.
<http://www.admin.ch/ch/f/rs/235_11/>

United Kingdom

Data Protection Act 1998, 1998 Chapter 29.
<http://www.hmso.gov.uk/acts/acts1998/19980029.htm>.

United States

Privacy Act of 1974, 5 U.S.C. § 552A.
<http://www4.law.cornell.edu/uscode/5/552a.html>

b. Identification of human remains

Australia

Coroners Act 1997 (Australian Capital Territory), No. 57, 1997.
<http://www.austlii.edu.au/au/legis/act/consol_act/ca1997120/>

Coroners Act 1993 (Northern Territory), No. 30, 1993.
<http://www.austlii.edu.au/au/legis/nt/consol_act/ca120.txt>

Coroners Act 1958 (Queensland).
<http://www.austlii.edu.au/au/legis/qld/consol_act/ca1958120/>

Coroners Act 1995 (Tasmania), Act 73 of 1995.
<http://www.austlii.edu.au/au/legis/tas/consol_act/ca1995120.txt>

Coroners Act 1985 (Victoria), Act No. 10257/1985.
<http://www.austlii.edu.au/cgi-bin/download.cgi/download/au/legis/vic/consol_act/ca1985120.rtf>

Coroners Act 1996 (Western Australia).
<http://www.austlii.edu.au/au/legis/wa/consol_act/ca1996120.txt>

Belgium

Loi sur les funérailles et sépultures, 20 July 1971.
<http://194.7.188.126/justice/index_fr.htm>

Canada

Civil Code (Quebec), L.Q., 1991, c. 64.
<http://www.lexum.umontreal.ca/ccq/en/index.html>

Act respecting the determination of the causes and circumstances of death (Quebec) , 1983, c. 41.
<http://publicationsduquebec.gouv.qc.ca/fr/cgi/frameset.cgi?url=/documents/lr/R_0_2/R0_2_A.html>

Exhumation Act (Newfoundland), R.S.N.L. 1990, Chapter E-18.
<http://www.gov.nf.ca/hoa/statutes/e18.htm>

Coroners Act (Ontario), R.S.O. 1990, c. C-37.
<http://www.e-laws.gov.on.ca/DBLaws/Statutes/English/90c37_e.htm>

France

Code pénal, Art. 225-17.
<http://www.legifrance.gouv.fr/html/frame_codes1.htm>

Code de procédure pénale (Partie législative), Art. 74.
<http://www.legifrance.gouv.fr/html/frame_codes1.htm>

Code des Communes, Arts. R361-15 *ff*.
<http://perso.libertysurf.fr/adroit/Interieur/html/commune.htm>

Code de la santé publique, Art. L1232-1 *ff*.
<http://perso.club-internet.fr/dominique.mathis/bdlr/codes/CSpub/CSPL123.html>

Ireland

Coroners Act, 1962.
<http://193.120.124.98/1962_9.html>

Malaysia

Local Government Act 1976, Act 171.
<http://www.putrajaya.gov.my/ldb/_private/Act_171/LGA_CONTENT.html>

New Zealand

Coroners Act 1988.
<http://rangi.knowledge-basket.co.nz/gpacts/public/text/1988/an/111.html>
<http://rangi.knowledge-basket.co.nz/gpacts/public/text/1996/an/117.html>

Switzerland

Code pénal, Art. 262.
<http://www.admin.ch/ch/f/rs/3/311.0.fr.pdf>

United States

General Laws of Massachusetts, Chap. 38: Medical examiners and inquests.
<http://www.state.ma.us/legis/laws/mgl/gl-38-toc.htm>

New York State Consolidated Laws, Executive, Art. 35: Division of Criminal Justice Services.
<http://assembly.state.ny.us/leg/?cl=39&a=63>

United Kingdom

Coroners Act 1988, 1988 Chapter 13.
<http://www.hmso.gov.uk/acts/acts1988/Ukpga_19880013_en_1.htm>

c. Protection of genetic information

Argentina

Ley 23511 - Banco Nacional de Datos Genéticos, 10 September 1986, Boletín Oficial, 30 September 1986.
<http://www.foroabogadossanjuan.org.ar/Leyes/Leyes_Nac/lc-10089.html>

Australia

Crimes Act 1914, Act No. 12 of 1914 (Part 1D - Forensic procedures).
<http://www.austlii.edu.au/cgi-bin/download.cgi/download/au/legis/cth/consol_act/ca191482.txt>

Crimes Amendment (Forensic Procedures) Act 2001, No. 22, 2001.
<http://www.austlii.edu.au/au/legis/cth/num_act/capa2001n222001384/>

Canada

Criminal Code, R.S. 1985, c. C-46.
<http://laws.justice.gc.ca/en/C-46/index.html>

DNA Identification Act, 1998, c. 37.
<http://laws.justice.gc.ca/en/D-3.8/text.html>

France

Code civil, Arts. 16 *ff*.
<http://www.legifrance.gouv.fr/html/frame_codes1.htm>

Code de procédure pénale (Partie législative), Art. 706-54.
<http://www.legifrance.gouv.fr/html/frame_codes1.htm>

Code de procédure pénale (Partie Réglementaire - Décrets en Conseil d'Etat), Arts. R-53-9 *ff*.
<http://www.legifrance.gouv.fr/html/frame_codes1.htm>

Switzerland

Ordonnance sur le système d'information fondé sur les profils d'ADN, 31 May 2000.
<http://www.admin.ch/ch/f/rs/361_1/>

Projet de loi fédérale sur l'utilisation de profils d'ADN dans le cadre d'une procédure pénale et sur l'identification de personnes inconnues ou disparues, 8 November 2000.
<http://www.admin.ch/ch/f/ff/2001/49.pdf>

Ordonnance sur le système de recherches informatisées de police, 19 June 1995.
<www.admin.ch/ch/f/as/2000/2951.pdf>

United Kingdom

Criminal Justice and Public Order Act 1994, 1994 Chapter 33.
<http://www.hmso.gov.uk/acts/acts1994/Ukpga_19940033_en_1.htm>

Criminal Justice and Police Act 2001, 2001 Chapter 16.
<http://www.hmso.gov.uk/acts/acts2001/20010016.htm>

United States

DNA Identification Act of 1994, 42 U.S.C. § 14132.
<http://www4.law.cornell.edu/uscode/42/14132.html>

General Laws of Massachusetts, Chapter 22E: State DNA Database.
<http://www.state.ma.us/legis/laws/mgl/gl-22e-toc.htm>

New York State Consolidated Laws, Executive, Art. 49-B: Commission on forensic evidence and establishment of DNA identification index.
<http://assembly.state.ny.us/leg/?cl=39&a=78>

4. Participants

Body	Function	Full name
Attorney General's Office (Argentina)	Prosecutor and Data Protection Expert	Ms Alejandra Gils Carbó
	Legal consultant (human rights and data protection) (United Kingdom)	Mr Douwe Korff
	Legal consultant (data protection in the medical and genetic fields) (Canada)	Mr Eugene Leon Oscapella
Office of the Federal Data Protection Commissioner (Switzerland)		Mr Kosmas Tsiraktsopulos
International Committee of the Red Cross	Head of the Advisory Service on International Humanitarian Law	Ms Maria Teresa Dutli
International Committee of the Red Cross	Legal adviser, Advisory Service on International Humanitarian Law	Mr Richard Desgagné