COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Strasbourg, 4 November 2010 T-PD-BUR(2010)12 FINAL

THE BUREAU OF THE CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA

(T-PD-BUR)

22nd meeting
15-17 November 2010
Strasbourg, G04

Study on Recommendation No. R (87) 15 of 17 September 1987 regulating the use of personal data in the police sector

"Data Protection Vision 2020 Options for improving European policy and legislation during 2010-2020"

By Joseph A. Cannataci

This contribution was written in a strictly personal capacity and does not necessarily reflect the official position of the Council of Europe.

Secretariat document prepared by
the Directorate General of Human Rights and Legal Affairs

10/31/2010

Council of Europe Recommendation R(87)15 & ETS Convention 108

Data Protection Vision 2020

options for improving European policy and legislation during 2010-2020

Joseph A. Cannataci

Data Protection Vision 2020

options for improving European policy and legislation during 2010-2020

1. Context of the Study

This study has been drawn up in the context of a consultancy contract between the Council of Europe represented by Mr Jörg Polakiewicz, Head of the Law Reform Department, Directorate of Standard Setting, Directorate General of Human Rights and Legal Affairs and Dr. Joseph Cannataci, Professor of Technology Law and Director of the Centre for Law, Information & Converging Technologies, University of Central Lancashire, United Kingdom, hereinafter referred to as "the Consultant".

2. Scope

The Consultant was requested to prepare a study on Recommendation N° R(87) 15 of 17 September 1987 regulating the use of personal data in the police sector and to suggest proposals for the revision of the above Recommendation. The Consultant was requested to identify, in particular:

> whether the current scope of application provides the necessary levels of safeguards for personal data processing in the light of emerging new actors involved in the prevention, detection, investigation and prosecution of criminal offences or the execution of criminal penalties as well as in the light of the use of new practices and technologies;
>
> the fields where specific problems may arise from the point of view of the application of data protection principles and, in particular, the field of the use of personal data in the police sector. The Consultant shall also consider to what extent the provisions of the Convention for Protection of Individual with regard to Automatic Processing of Personal Data (ETS No 108) and the abovementioned recommendation cover the current preoccupations and expectations.

In his report, the Consultant was required to include an appendix containing a set of proposals for amendments to the existing provisions or for drafting additional provisions.

3. Structure of the Study and Background information

Given the constraints imposed by the contractual word limit, the main body of the study will only deal with background information and data where these are immediately pertinent to a point of analysis and/or a recommendation being made. The Consultant shall assume that the readers of this present study are familiar with three other recent studies that he has authored. The first of these, attached to this study as Appendix 2, focuses on Recommendation R(87)15 and its role in a European context to the coming into force of the European Union's Data Protection Directive in 2006. The second background

paper included here as Appendix 3, identifies the risks to privacy in police uses of smart surveillance technologies including MIMSI and sets these in the context of the European Union's Council Framework Decision/977/JHA/2008. The third (Appendix 4) deals with the notion of purpose in data protection law. Taken together, these three background papers should serve to bring relative newcomers to the area up to date with a number of privacy risks and relevant developments in police use of personal data to 2010.

4. Approach taken by the Consultant–R(87)15 & Convention 108 in context

The overall approach taken by the Consultant is that although the brief is understandably focused on Recommendation R(87) 15 and Convention 108, the efficacy of these two legal instruments cannot be measured properly if considered in a vacuum or if they are taken out of their proper context in European and international law. The proposals and recommendations made by the Consultant shall therefore at each step, bring to bear knowledge of developments in other areas of privacy and data protection law outside the immediate texts of R(87)15 and Convention 108 but which would have a bearing on any attempts at improving these important instruments devised by the Council of Europe.

5. Substantive and Procedural Assumptions

The analysis undertaken in this study will also depend on two sets of assumptions, one substantive, the other procedural.

5.1 The substantive part of the study is based on the following assumptions:

a. That security is and will remain a fundamental requirement for stable and prosperous societies as well as a priority expectation of the citizens in those societies
b. That the expectations of citizens may fluctuate but include a heightened expectation of privacy tempered by a willingness to indulge in/permit a privacy-benefit trade-off in lifestyle choices especially vis-à-vis all the technologies that make life more convenient
c. That convenience remains the key to both citizens and police/security forces when it comes to choices about technologies – they will not choose to use a technology unless it makes life easier but if the technology exists and is widely adopted and it is convenient to tap into even for police/security purposes then public-private interaction in this sphere may be expected to grow
d. That technologies which are "better-by-design" and which incorporate the principle of "privacy-by-design" are more efficient and cheaper and more cost-effective than technologies where privacy considerations are bolted-on as an afterthought
e. That the rule of law is an essential part of an integral approach to security in society whereby the law provides the rules which facilitate, promote, create and enforce the right environment where the right balance is struck between individual privacy, convenience and public safety and security.

f. That if the citizen perceives that he or she is truly respected by both the public and private sectors then both security and profitability may be maximised through the right blend of legislative, policy and technological solutions

5.2 The procedural assumptions include:

a. That any changes proposed either to Convention 108 or to Recommendation R(87)15 would need to be subjected to co-ordination procedures by the 27 member states of the Council of Europe that are also members of the European Union. In other words changes to Convention 108 and R(87)15 would need to be compatible with the changes to the EU's own data protection regime which itself is currently under active consideration.
b. That any changes made by the EU to its data protection regime between 2010 and 2015 would strengthen the principles and operation of EU Directive 1995/46/EC but do so with at least one eye open to these possibly forming a consensual basis of future co-operation with the United States of America and this following the preliminary consensus achieved by the High Level Contact Group and the USA as declared on 28 October 2009 (attached here as Appendix 5).
c. That the EU would give added weight to the opinion of the European Data Protection Supervisor that existing agreements with the United States relevant to police/security use and exchange of personal data be consolidated into one agreement and not remain in the current state of a number of disparate arrangements which may occasionally give rise to risks and inconsistencies.
d. That, following the coming into force of the Lisbon Treaty, the EU's Council Framework Decision 977/JHA of 2008 (attached here as Appendix 6) will need to be revised in order to be made more compatible with, and possibly incorporated into a new version of, EU Directive 46/95 and that when this would happen the substantive content of CFD/977/JHA/2008 would be applied to all utilization of personal data for police purposes and not merely for the exchange of criminal justice sector data between EU member states
e. That, once the EU reviews and in some places possibly re-writes or expands EU Directive 1995/46/EC and combines this with a revised version of CFD/977/JHA, this would form the basis of the EU's negotiating stance both within the Council of Europe and also with all non-European states who would wish to exchange personal data both within the police sector and outside it.
f. That a growing number of states outside Europe would wish to establish common ground with the "European Data Protection Club" and that a truly international instrument endorsed by a number of non-European states as well as the overwhelming majority of the member states of the Council of Europe, would stand a much better chance of attracting international consensus.
g. That the Council of Europe would wish to learn from past experience and largely that countries would not sign up to an international multi-lateral treaty such as a Convention simply because the Convention contains sound principles but also because they started "owning" the treaty since they were involved in its drafting from the very beginning. The different take-up rate by major non-European states of Convention 108 and e.g. Convention 185 (The Cybercrime Convention) as well as other similar instances in international law should serve as a reminder that one can ignore certain major players at drafting stage only at one's peril.

h. That the Council of Europe would wish to learn from past experience that it needs to address the inherent weakness of R(87)15 which, like other recommendations in the field of data protection suffers from the nature of the legal instrument chosen: a Recommendation i.e. an optional extra as opposed to a protocol to a treaty which, once signed would gain binding force within the member states.
i. That the Council of Europe would wish to seize upon the present state of international relations (especially between the EU and the United States of America) as a useful opportunity to play "honest broker" and involve these and other states in a wholesale review of R(87)15 and Convention 108.

6. "An inalterable necessary minimum" – enduring but too minimalistic?

The first consideration that is being made is whether the key conclusion reached in the 1993 review of R(87)15 is still valid? For all the reasons expressed in the three preceding reviews of R(87)15 this Consultant endorses the view that the provisions of R(87)15 remain "an inalterable necessary minimum". It is important however that in 2010 this view is immediately qualified in the following manner: the provisions of R(87)15 and especially those which reinforce the principle of purpose even for police and security forces are the absolute minimum and are inalterable only in the sense that they should not be reduced or in any way diluted. This study will however ask the complementary questions: "Has the passage of 23 years shown that "the necessary minimum" is too minimal? Do the changed circumstances of 2010 make it advisable to strengthen and expand the provisions of both R(87)15 and Convention 108? The answers to both these questions will be an unqualified "Yes" and the reasons for this will be summarized in a separate section below.

The enduring influence of R(87)15 lives on well past the background analysis provided in Appendixes 2 , 3 and 4. The latest example of this is probably Romania's Law nr. 238 of the 10/06/2009[1] which basically takes R(87)15 and transports it lock, stock and barrel into Romanian law less than a year before this present study was commissioned. Indeed so much is this the case that the new Romanian law which came into effect on the 18th June 2009 continues to make the distinction between collection and processing of data that largely disappeared when collection was subsumed by the EU's definition of "processing" in EU Directive 46/1995. Apart from the fact that certain definitions in this new 2009 Law may be out of synch with other definitions in the rest of the corpus of Romania's data protection laws, it does raise the question as to why R(87)15 provided the model to an extent which seems to have largely ignored the immediacy of Council Framework Decision CFD/977/JHA[2] The basic question being asked here is not "Is R(87)15 still useful ? Clearly, as the new Romanian Law 238 shows, it is. The question is "Is it useful enough for the circumstances of 2010? Can a revised, expanded R(87)15 do better?"

[1] Published in Monitorul Oficial, Partea I nr. 405 of the 15/06/2009 and attached to this report as Appendix 7.

[2] The extent to which Romania's Law nr. 238 of the 10/06/2009 complies with and implements Council Framework Decision CFD/977/JHA is the subject of a separate detailed study in preparation.

7. Changed circumstances - 20 Major Differences between 1987 and 2010

Before moving on to examine options for building upon R(87)15 and Convention 108), it is worth considering some of the relevant major differences between 1987 (indeed 1981) and 2010:

1. All forms of personal computers, desk-top, notebook and netbook ,are now ubiquitous all across European states and in a rapidly growing number of states outside the Council of Europe;
2. These personal computers in Europe and many outside Europe are now largely interconnected through the Internet and the World Wide Web;
3. These billions of interconnected personal computers have been joined by further billions of mobile phone devices many of which are the meeting place for three converging digital technologies: telephony, imaging (still and video cameras), e-mail and internet -apable hand-held computers;
4. The transactional or traffic data generated every day in 2010 (but by comparison quasi non-existent in 1987) by these personal computers and mobile telephones/devices through Internet browsing, e-mail, e-commerce, e-government, e-health, social-networking systems, land-line /mobile phone calls and SMS texts, have brought into being trillions of transactions capable of profiling citizens as well as billions of communications replete with voice or text or image content some of which could constitute personal data in terms of data protection law;
5. All the data outlined above, personal or otherwise, flow across borders (European and non-European) instantaneously and, mostly without explicit ad hoc prior permission;
6. The exponential increase of personal data since 1987 in content and transactional data generated on/by PCs, the Internet and mobile phone devices has been matched by an exponential increase in overt surveillance especially by closed-circuit television (CCTV) in both public and private places which generates even more personal data.
7. The data generated by CCTV and other imaging techniques mentioned above as well as land-line and mobile telephone devices has moved from analog to digital platforms which facilitates the automated analysis of such data.
8. The sheer quantity of the trillions of images and data files generated every day in the new systems described above put them beyond the viable reach of cost-effective analysis by human beings and therefore provide a fertile area of application for automated recognition systems of the type regulated by Art 2.3 of R(87)15 and Art 7 of CFD/977/JHA/2008 (see Appendix 3 for relevant analysis). This means that, because of technological advances, both the increased capacity in producing more and more personal data as well as the improved capacity to sift through such data in an automated manner will mean that automated decision-making will be a much greater issue in data protection especially in a police surveillance context than it has been at present or to date.
9. Public and private databases containing personal data in sectors as diverse as e-government, health care, social welfare, insurance, statistics and banking have continued to proliferate in a way where their increased connectability and frequent news of losses of personal data found in these databases point to a significant dimension of risk that has not yet been brought under control.

10. All of the personal data sources indicated above are in2010 increasingly being interconnected through the MIMSI systems (Massively Integrated Multiple Sensor Installations) described in more detail in Appendix 3 already deployed by police forces in the United States and China with probable spread to police and security forces across Europe during the period 2010-2015. Yet the safeguards being put into place by police forces in such instances[3] do not meet the standards set by R(87)15 in 1987 let alone the even stricter standards that may be required.
11. In 1987 there existed a European Economic Community of 12 member states with no jurisdiction over justice, police and home affairs. In 2010 this has metamorphosed into a formidable bloc of 27 countries which after the Maastricht treaty of 1992 became the European Union and which after the coming into force of the Lisbon Treaty on 1 December 2009 now counts justice, police and home affairs amongst its competences. The reality of 2010 (as seen in the recent Feb-July 2010 debacle over SWIFT data as well as in the 2009 HLCG agreement on data protection principles) is that the USA first seeks to negotiate with the EU as a collective entity on matters of data protection, often in preference to bilateral agreements with the very member states of the EU. The Council of Europe is not taken into account in this scenario.
12. The European Union has meanwhile established its own corpus of legislation relevant to the protection of personal data (notably Directive 1995/46/EC and Directive /2002/58/EC as well as CFD/977/JHA/2008) or which may actually negatively impact its protection (notably the 2006 Data Retention Directive). This development has spurred non-EU states to find ways of enabling their business to exchange personal data with EU-based entities and although devices such as Standard Contractual Clauses are being used, dissatisfaction is often expressed at the current regime while the take up-rate on the EU's own "adequacy" procedures has been very low.
13. The internationalization of activities by terrorist groups and organized crime especially after the 9/11 attacks in the United States has led to increased and huge pressure on national police and security forces in European states to exchange personal data with police and security forces in other European as well as non-European states for the purposes of prevention, detection, investigation and prosecution of offences.
14. Both the existence of CFD/977/2008/JHA (i.e. the resultant pressure on 27 of the Council of Europe's 47 states to change their laws to conform to this CFD) as well as the inadequacies of CFD/977/JHA (particularly the fact that it currently does not regulate the processing of personal data within-as opposed to between- EU member states) and the fact that CFD/977/JHA itself has also been overtaken by events (largely the coming into force of the Lisbon Treaty mostly abolishing the old exclusions reserved for the Third Pillar) leaves a regulatory vacuum that needs to be filled quickly with solutions acceptable to both EU member states and the wider Council of Europe membership. This could be an opportunity for the Council of Europe to resume its leadership role in data protection law especially given the recent problems for exchange of personal data for police purposes, including the issue of US access to SWIFT data which led to disagreement between the EU and the United States in February 2010 and has only been settled on an interim basis in July 2010.

[3] See Appendix 3 for a summary analysis of eg. the safeguards introduced by New York City Police.

15. We have witnessed in daily practice a dilution of the traditional safeguard of explicit and informed consent by the data subject to processing of his/her own personal data. This is especially evident in on-line social networking sites and click-wrap agreements where empirical evidence is increasingly showing that data subjects are being led into explicit consent in a situation where one ticks a box to obtain access to a service but where the privacy standards may be both inadequate and constantly changing. The consent obtained may be explicit enough but it is probable that in most cases it is nowhere near being truly informed or free.
16. We have likewise witnessed a growing disregard, in practice, and especially in some European countries more than in others, for the cardinal principle of purpose enshrined in Convention 108. The role of the EU's Data Retention Directive in this regard is examined in some detail in Appendix 3 while the UK situation in particular regarding purpose is analyzed in more detail in Appendix 4.
17. Police use of on-line searching of computers without prior judicial authorization has on the 27 February 2008 been declared unconstitutional in a leading European state like Germany where the Constitutional Court has recognized the "Right to on-line digital privacy"
18. The increased use of the Internet to reveal details about private lives of individuals and other forms of personal data leads one to question the absence of effective sanctions in such instances and to query the possibility/desirability of criminalization of sanctions for breach of privacy as well as neighbouring rights in the field of *lex personalitatis* such as on-line defamation.
19. The number of adhesions to or implementations of both Convention 108 and R(87)15 appears to have plateaued and this in spite of the clear wish of a number of non-European states to be part of an international consensual agreement where data protection issues are properly regulated. Some blunt questions need to be asked and answered in this context. Learning from the case of Convention 185, to what extent would Convention 108 have been a more attractive proposition to non-European states had some major players like the United States, Canada, Japan and, increasingly, Brazil, China and India already been on board?
20. The key tools which enabled the Council of Europe to establish a clear and inspirational lead in the field of data protection for over 20 years no longer exist. Between 1976 and 2002, the Committee of Experts on Data Protection (CJ-PD) and its various Working Parties produced Convention 108 and a number of increasingly useful recommendations. While the T-PD has attempted to soldier on valiantly, the recent disappearance of the CJ-PD has left a huge vacuum. In order to re-gain the momentum that now risks being lost it is essential that the Council of Europe gives priority to data protection in the Knowledge Society and shows this resolve by again committing adequate financial resources to the continuation of the work of the CJ-PD. This is especially the case where, as may be seen, for an interim period of at least ten years until 2020, the T-PD may be perceived externally as being *partem in causa* with a remit and resources which are insufficiently wide to cover the vast ground that data protection has become in the 21st Century. This caveat made, it is perfectly possible that the work of the CJ-PD may actually be continued by the T-PD but to do so it would still require a significant increase in resources.

These, in summary, are therefore some of the relevant changes which are the hallmark of the situation in 2010 as opposed to the situation obtaining when Convention 108 was opened for signature in 1981 or when R(87)15 was approved in 1987 or even at key points of previous review like 1993 and 1998. It is against these changes that R(87)15 and Convention 108 need to be examined for weaknesses and thus possible areas where they may be strengthened otherwise it is feared that they may risk moving from a position of inspirational immediacy to one of historical importance but contemporary irrelevance.

The major changes outlined above suggest that the risks to personal data have multiplied exponentially while the Council of Europe's regulatory framework has not moved on despite a significant shift in proportionality between risk and regulation. It is submitted that in 1981, 1987, 1993 and 1998 it was wise to be cautious and to adopt a convention which was generic and recommendations which were non-binding as European states eased themselves into the Information Age and the Knowledge Society. The deployment of the technologies catalogued above – and the resultant data protection risk – was then significantly lower while the take-up rate of these Council of Europe legal instruments by European and non-European states was then relatively untested. A quarter-century has now gone by and a number of developments, some predicted, some less so, have come to pass. The Council of Europe has new realities to deal with and it is this Consultant's view that Convention 108 and Recommendation R(87)15 are no longer a proportionate response to the levels of risk to personal data which exist today (and some of which are outlined in Appendix 3 and Appendix 4). The levels of risk are now significantly higher and they call for levels of legislative response which are binding upon European states and which are sufficiently detailed to be really useful for the practitioners in the field. This is why in 2010 it is no longer possible to return with a result similar to the reviews of 1993, 1998 and 2002 which basically said "leave well alone". It is not "well" any more. The number of countries adhering to or implementing both Convention 108 and R(87)15 has now tailed off, a number of significant risks (eg MIMSI, consent, etc.) are not being adequately tackled, and non-European states are looking for inspiration and possibly agreement elsewhere.

It is counter-intuitive that this should be so. At no time as in 2010 has the need for processing and exchange of personal data by police forces, especially in the face of internationalized, globalized terrorism, been more pressing with the concomitant requirement to have adequate data protection safeguards in place for such processing. At no time as in 2010 has the need of processing and exchange of personal data by businesses located outside Europe created as much of a demand for a platform for an international consensus on data protection standards as that potentially afforded by Convention 108. Terrorism and personal data exchange for business reasons are international concerns and not merely European issues. Yet the Council of Europe is not dealing with a queue of countries knocking at its doors wishing to ratify Convention 108. Nor is it witnessing adoption en masse of R(87)15 and its further development across European and non-European states. So something must be wrong. Something must be making these legal instruments less attractive and useful then their authors wished them to be. It is therefore logical that the next step in this study would be to identify the weaknesses which may have contributed to the waning success of the once hugely successful and basically still valid Convention 108 and Recommendation R(87)15.

8. The major weaknesses of R(87)15 in 2010: Procedural & Substantive

With the benefit of hindsight and in the view of changed circumstances it is possible to discern two main categories of weaknesses in R(87)15

8.1 Procedural: There are four major "procedural" problems with R(87)15.

The first is that it is a non-binding recommendation and as with many other optional safeguards it was omitted or ignored by a number of European and non-European states.

The second is that is a disparate part of a codex which has over the years possibly become too loose. How many legislators and data protection officials across Europe bear in mind or even know of the Council of Europe's ten recommendations on data protection ranging from health care to insurance through statistics, social welfare, marketing, media, police, means of payment, employment and the internet? The solution therefore would seem to be the revision of the existing recommendations including and perhaps especially R(87) 15 and their integration into Convention 108 or its successor as an additional protocol. This should serve to provide a more coherent and useful approach to the realities of protecting personal data in the 21st century by providing a common binding approach to the use of personal data for police purposes by member states of the Council of Europe.

The third and possibly most significant weakness is that of "ownership". Despite observer states having been present at their inception, Convention 108 and R(87)15 remain solidly European legal instruments which are attempting to regulate a situation which has irreversibly gone global and which therefore requires a global consensus. European legal instruments may have an impact on the way that personal data are collected and processed in Europe but are of limited usefulness in the globalised world which is cyberspace and/or where personal data may be required to be exchanged to prevent, investigate or prosecute terrorist attacks in Mumbai, Nairobi, Yemen, Beijing or Sao Paolo. For Convention 108 and R(87)15 to become truly effective rather than symbolic they must be "owned" – and preferably re-conceived by a far wider group of states than those which are members of the Council of Europe.

The fourth weakness is the lack of an inter-governmental or supranational Supervisory Authority which would have the remit and the competences to audit the standards of data protection maintained by Police and Security forces. This is a hugely delicate matter which for some time has been the elephant in the room that nobody wishes to see. The United States has learnt from bitter experience in this regard. In a knee-jerk reaction to the 9/11 incident it ushered in the Patriot Act which for the best part of 5 years permitted U.S. police and security forces to obtain data about private citizens without sufficient oversight, whether judicial or otherwise. This situation was remedied in 2006 when an oversight function was allocated to the US Dept of Justice OIG (Office of the Inspectorate General). The latest reports published in January 2010 brought to public attention more than 2,000 cases of abuse by the FBI in its disproportionate quest to obtain personal data. If there were to be a scale of difficulty for changes to data protection in the police sector a proposal to create a supranational supervisory authority would probably be ranked as the most radical since the rivalry between different police and security forces within the same state are legendary. Compound that inter-service rivalry with issues of sovereignty and

nationalistic chauvinism and the prospect would seem nightmarish. That however remains the ideal scenario: a joint standing international commission blending the skills of experienced police-persons and data protection/ICT experts which would have the authority to audit and report upon the data protection standards as applied in practice of any given police force within Europe or indeed in any country party to a police data-exchange agreement.

8.2 Substantive: The principles of both Convention 108 and R(87)15 remain sound but are expressed in terms which are now occasionally too generic to be immediately useful in many situations. They now require a more detailed development while remaining as technologically neutral as possible under the prevailing circumstances. One of the solutions contemplated under the Procedural weaknesses above would basically incorporate R(87)15 into Convention 108 (or its successor) and make it binding. Having made the basic tenets of R(87)15 explicit and binding, what would be useful to police and security forces are guidelines or sets of guidelines which are detailed, clearly spelt out and legally enforceable. This is perhaps where a case-study of substantive rules may be useful. The guidelines (contained in Appendix 7) adopted by the New York Police were hailed (by the New York Police) as being first-of-a-kind though their various deficiencies have already been noted in Appendix 3. It is not necessarily all of their content which should be considered to be "good practice" or "best practice". What should be considered is the example they set in defining purpose, the level of detail (which is sometimes adequate and at others too minimalistic or "elastic") and certain procedural provisions. Their status as non-binding guidelines is certainly not commendable.

What is required are legally-enforceable regulations (not guidelines) which would be common to all police forces in Europe and preferably beyond. These regulations should do that which the substantive parts of R(87)15 currently do not cover. They should for example contain sufficient detail as to how to handle personal data in MIMSI-type situations. Whereas R(87)15 may eventually be incorporated into Convention 108 or its successor either in the main body or as an additional Protocol, the detailed procedural regulations could be attached in a manner susceptible to easy and possibly relatively frequent amendment in order that they may be up-dated as and when circumstances and technological innovation require.

The substantive issues to be addressed by these detailed legally enforceable regulations (even if sometimes only in template or "tool-kit" form) will not here be dealt with in the form of detailed drafting proposals but rather an outline of criteria (some of which are already partially addressed in outline form in R(87)15) to be developed by international drafting groups and should normally include:

1. A detailed definition of what the technological system utilized by the police force/agency comprises of (eg. CCTV, sensors, deep-packet inspection etc.) This should also include a clear and unambiguous definition of whether the system comprises only of police-owned or state-owned devices or also as to whether the system may access or otherwise connect to devices and databases owned and/or operated by other government agencies as well as private companies or individuals.

2. A detailed specification of the purpose for the collection of personal data by the particular police or security agency clearly identifying the threat to safety and public security that the system is designed to protect against in a proportionate manner.
3. A prohibition for any use (further processing) or further communication of personal data save for the specified purpose or one compatible with that specified purpose.
4. A detailed exhaustive definition of what constitutes areas in real space and in cyberspace where a legally protected expectation of or right to privacy may reasonably be said to exist.
5. A detailed exhaustive list of who inside the police force is to have access privileges to the system and as to what level.
6. A detailed exhaustive list of which automated recognition technologies (face, gait, RFID or otherwise) may be utilized by the system or the utilisation of which is prohibited together with the safeguards being put in place to ensure that automated decisions do not prejudice individual data subjects.
7. Clear functional specifications for the system design which should specifically cater with stringent security measure for the system's protection from both internal and external unauthorised access as well as a compulsory unalterable audit trail for all transactions. These specifications should also contain a clear procedure for how, when and by whom the police system may be interconnected to other systems.
8. A clear procedure for what, when, how, by whom and to whom personal data may be communicated by the police agency to third parties.
9. The length of time for which personal data may be stored and clear procedures to be followed if this time needs to be extended further.
10. A clear indication of the oversight authority entrusted with independent scrutiny of the personal data handling activities of the police agency including a predictable regime of sanction to which a police officer/operator may be subjected in those cases where these regulations are breached.

9. Options for future amendments and expansion of R(87)15

The options open to the Council of Europe may possibly be categorized into four, each one more radical and ambitious than the previous one. These options are designed to tackle the procedural weaknesses identified in the analysis in Section 8 above and may generally be seen as a graded approach to addressing one, some, most or all of these procedural weaknesses. It is assumed that the substantive weaknesses would be addressed through apposite drafting in any one of the four options chosen.

1. Follow the opinion of the European Data Protection Supervisor and other commentators and "legislate R(87)15 into European Law" through the "simple" expedient of incorporating it into an additional protocol to Convention 108 and encouraging member states to ratify this additional protocol. This has the advantage of relative simplicity but remains a European solution for what has already become a matter of global concern. While doubtless improving matters within Europe and helping to counter the current vacuum created by the non-applicability of CFD/977/JHA/2008 to intra-national uses of police data AND deliver a model law providing

safeguards where automated decision-taking is involved, this would not deal effectively with the pressing need of an international solution to exchange of personal data used for police purposes outside Europe. This process would last at least 24-36 months since it would also need to take on board further changes to R(87)15 as suggested in the substantive part of the "weaknesses" section above. This process could also benefit from emerging empirical research within European projects which deal with automated recognition[4].

2. The second option would be to carry out step one above as the first part of a systematic approach to including all of the Council of Europe's Recommendations on Data Protection and legislating them into being as integral parts of Convention 108 or additional protocols. This would be a process whereby review and integration of the existing texts could be done concurrently to a certain extent but would certainly take 60-72 months overall (depending on how much resources are committed to the task). Priority, after R(87)15 should perhaps be given to medical data R(97)5, given the immediacy of the issues tackled therein. This option has the advantage of tackling the first and second procedural weaknesses and tidying up the European codex on data protection law but has the significant disadvantage of remaining a purely European approach to what is essentially a set of global issues.

3. The third option would be to keep Options 1 and 2 above as a "Plan B" or "Plan C", i.e. as a secondary fallback position and instead embark on a bolder strategy aimed at creating a new international consensus on data protection. The Council of Europe would, in this case, "bite the bullet" in the same way that it did with Convention 185 but in an even wider manner and invite a number of countries to a Working Party or special ad hoc Committee, possibly but not necessarily under the aegis of the T-PD. The non-European countries should include (in alphabetical order) Australia, Brazil, Canada, China, India, Japan, Korea, New Zealand and the United States. Representatives of the African Union, the Arab League should be invited while a judicious selection of Council of Europe member states should help ensure representation of the heterogeneous and leading legal cultures within the 47. In this option the name of the new Working Party or Committee may have some significance for at least some of its membership. Essentially this would constitute an "International Committee for a Treaty on Privacy & Data Protection". In its lobbying as well as in its letter of convocation the Council of Europe should be frank about the values but also about the inadequacies of its own existing instruments. There can be no question as to Convention 108 and R(87)15 and the other recommendations being the starting point for the Council of Europe's negotiating position but it would be salutary indeed to invite all the nations indicated to the table and face three basic sets of issues:
    a. There are at least 20 major ways in which the world has changed over the past 25 years and technological advances have meant that there is much more personal data out there and it is at significantly higher risk with the available evidence pointing to citizens being increasingly concerned about this situation.

[4] Like, for example, the SMART project financed under the FP7 programme of the European Commission

b. Given the internationalization of criminal activity and terrorism it is advisable to agree to a consensual position which strikes the right balance between the protection of personal data and the exchange of personal data across borders for the purposes of prevention, detection, investigation and prosecution of crime.
c. Given the internationalization and globalization of commerce and industry in a way which requires personal data to be moved about the planet irrespective of it being inside or outside European borders it is advisable for a consensual position on general standards of data protection to be agreed in a way which would facilitate transborder data flows, simplifying procedures and reducing costs for business while at the same time maximizing reciprocal protection and high standards of protection of personal data wherever that data may happen to be processed.

In this way the Council of Europe could build upon the closer-than-ever positions arrived at on EU-US consensus in the 28 October 2009 HLCG on data protection. Most of the principles agreed in that statement resonate with the principles of Convention 108. The NDPC would be an opportunity to bring people around the table and make everybody, European and non-European, own the process which could possibly lead to agreement. The European position would be clear "We want to improve the position in Europe but the issues surrounding the exchange of personal data especially for police purposes are global and not merely European. We already have Convention 108 and EU Directive 1995/46/EC and a host of recommendations and we can continue developing those legal instruments on our own but that in itself would not facilitate the exchange of personal data either for business or for police purposes which today are global issues. So we thought that it may be a good idea to invite everybody around the table and build up a consensus on these issues, all of us learning from the lessons of the past 25 years. We are ready to come up with a wholly new binding international instrument which would improve upon everybody's present position". Some countries and especially perhaps China and the USA may have some difficulties in signing up to some principles immediately but if the negotiations are handled skillfully the base positions may not be as far apart as people may think. There is of course, the possibility that this attempt to create increased international consensus will fail partially or wholly but we would not know unless we would have tried. If it comes off, like the Cybercrime Convention, it would be a significant step forward on many fronts. If it does not come off then one can always move to "Plan B" which could be, rather than have an all-embracing 2010 version of Convention 108 suitably revised in its detail (though not in its basic principles which would be retained as a minimum position), why not attempt to breathe life into the 1992 idea of having a separate convention which deals exclusively with data protection and exchange of personal data used for police purposes. This is not offered as a preferred option since this would leave unregulated the issue of transborder exchange of personal data for business reasons which, in point of fact, constitute the vast bulk of transborder flows of personal data whereas those transferred for police purposes are a tiny fraction of the entire whole but this Consultant is duty bound to point out that it may still exist as an option.

4. The fourth option would be to achieve option 3 above but with an added bonus i.e. the creation of a supranational authority with the competences and the remit to audit police forces in their use of personal data. This innovation would be the data protection equivalent of "the impossible" achieved when sovereign European states agreed to subject themselves to the jurisdiction of the European Court of Human Rights. Perhaps even more difficult since this touches on police uses which may be important for national security (or alleged to be so). This is a task which is so ambitious that it needs to be hived off from the option 3 above which is still achievable in most of its aims without necessarily having the creation of a supranational authority which would have oversight of what police forces are up to on the data protection front . (In Option 3 there would be the possibility of deferring such an oversight function to a national independent authority or judicial entity).

10. Conclusions

This report has referred to the background of R(87)15 and the risks prevalent in 2010 which are matters largely covered in Appendixes 2,3 and 4. After indicating the substantive and procedural assumptions on which the analysis would be based, this report summarized 20 major relevant changes that have occurred between 1987 and 2010. When considering these major changes, the report concludes that while the principles of R(87)15 remain valid and useful, they are formulated in a non-binding, sometimes insufficiently detailed way which significantly inhibits this usefulness. The major societal and sectorial changes outlined in this report suggest that the amount of personal data and the risks of abuse of this data have increased significantly and that Convention 108 and Recommendation R(87)15 are no longer a proportionate response to the levels of risk to personal data which exist today (and some of which are outlined in Appendixes 2, 3 and 4). The levels of risk are now significantly higher and they call for levels of legislative response which are binding upon European states and which are sufficiently detailed to be really useful for the practitioners in the field. The report then identified a number of procedural and substantive weaknesses in R(87)15, underlining the fact that in their current form these two legal instruments are unlikely to provide an attractive platform for the international consensus in data protection which is sorely needed especially vis-à-vis non-European states. The report concludes by identifying four main options for follow-up action which would appear to be available to the Council of Europe should it wish to address these weaknesses.

As specified in the brief, the recommendations of the Consultant are contained in Appendix 1 attached to this report.[5]

[5] I conclude also with an apology to all my colleagues and friends in data protection agencies and police forces around the world. If their system is an example of good practice or even a beacon of enlightenment and I have not cited it here it is not because I am questioning its validity in any way. It is because of the severe restrictions on space that this report permits. I would hope to compensate for this in a more detailed study for publication purposes and would be grateful if comments, suggestions and examples of laws, regulations, subsidiary legislation and good practices were to be sent to me at joe.cannataci@yahoo.co.uk

Appendix 1 - Recommendations

1. It is recommended that the Council of Europe pursues Option 3 identified in Section 9 of the main body of the report to which this Appendix is attached and which for our purposes here will be called **"New Data Protection Convention" (NDPC)** which would also incorporate operative and expanded content of R(87)15. As indicated in Section 9 of the main report it is essential that the Committee responsible for drafting the NDPC would invite as full members several non-European countries including (in alphabetical order) Australia, Brazil, Canada, China, India, Japan, Korea, New Zealand and the United States as well as representatives of the African Union, APAC and the Arab League. Not having this broad membership would defeat the primary purpose of selecting Option 3 which is to attempt to create the broad consensus reached by, for example ETS 185 but never by ETS108. The other reasons for recommending this route of action are the following:
   a. By opening a new international forum aimed at producing a new multilateral treaty on Data Protection the Council of Europe leaves Convention 108 and R(87)15 intact as a fall-back position. This is a lower-risk route than immediately opening the debate on Convention 108 and R(87)15 themselves which many European experts fear would re-open a Pandora's box at any event. If the initiative aimed at broadening international consensus on data protection is successful and the new treaty reaches the desired level, then the European partners may decide that this new Treaty supersedes and replaces Convention 108. If the NDPC project fails completely or does not reach the desired levels then the European states may opt to instead further develop Convention 108 by integrating R(87)15 into it possibly through the form of an additional protocol. Option 3 is therefore a low risk route to the maximum possible useful gains for the protection of personal data internationally.
   b. In a world where personal data has gone global it is for the time being unlikely that minor or major amendments to the existing R(87)15 or Convention 108 would achieve the desired goal of establishing common data protection standards that are respected world-wide. In other words it is unlikely that, after having stood on the sidelines for a quarter of a century those countries which have not implemented R(87)15 voluntarily or ratified Convention 108 are now suddenly going to do so because some tinkering is done with some of the articles of these instruments in their current form. By being offered the opportunity to co-author a completely new, more comprehensive treaty, non-European states (and especially the established and emerging major players) would be able to find and assume the ownership of the legal instrument that they could never have or could find in either R(87)15 or Convention 108. This means that Option 3 is a higher-probability of success route to attracting international consensus on data protection than continuing to hope that this can be achieved through the existing R(87)5 and Convention 108.
   c. Option 3 would build on both the consensus emerging from the HLCG (High Level Contact Group) – Agreement of 28 October 2009 and the solid foundations provided by the principles and logic of Convention 108. It would also offer the opportunity to achieve a *de facto* **Consolidation of the existing European regulatory framework** – The current

framework in Europe is provided by legal instruments conceived and promoted by the Council of Europe and the European Union. A number of these are inadequate and are currently under revision. Apart from improving the chances of attracting a wider international consensus, the NDPC would provide an opportunity to comprehensively review the relevant output of these two inter-governmental organizations and integrate them into a document which is far more coherent and cohesive than that obtaining presently. The NDPC could be used to effectively flesh out a number of existing provisions of Convention 108 in a technologically neutral way which might still be acceptable to a wider international consensus than that actually enjoyed by Convention 108.

d. The most obvious means of doing this would be to elaborate regulations consistently with the very spirit and logic of existing data protection law i.e. the fundamental principle of purpose. This may be achieved by amplifying the provisions of Convention 108 in the NDPC in a way whereby its applicability would be further specifically defined on a sector-by-sector basis depending on the purpose for which the data is collected, with the first of these sectors being that of police as covered by R(87)15. This approach has a number of benefits in that it may be incremental and also permit the Council of Europe to build on other invaluable work already carried out in the past by its internal organs and especially the Committee of Experts on Data Protection (CJ-PD). In this respect the Council of Europe may contribute significantly to the work of the Committee responsible for drafting the NDPC (and often lead the way) by taking the substance of a number of its Recommendations which currently may have wide consensus but are not legally binding and now effectively developing them further, and integrating them into the corpus of the NDPC.
e. This ambitious but necessary programme is not something that should be attempted in one go. The Committee entrusted with drafting the NDPC would be well advised to devise/adopt an architecture where the main body of the new Treaty would contain the basic provisions on which there is wide consensus and then be deliberately designed to be expanded through a mechanism such as an Additional Protocol (which is more flexible for opt-in/opt-out issues for some countries and which seems to have worked in a number of other cases including ETS 185). This modular approach to treaty building would mean that, for example, after the NDPC main body is completed and gradually ratified, the first two sectorial modules embarked upon could be those covering priority areas such as police and health care. These sectorial modules could be drafted through setting up a number of working parties working in close collaboration with e.g the EU's Art 29 Committee, with each WP focusing on a particular sector. Eventually, it would then also set up Working Parties for important areas not yet tackled by the Council of Europe and thus provide for incremental protection in a number of sectors. Much of this work could easily be achieved within 24-36 months, especially in those sectors where much European-wide and/or international consensus has already been created. In other sectors the detailed regulation could follow later after sufficient research, drafting, consultation and discussion, a process for which one could easily envisage an overall duration of 5-10 years. In this sense, for example, the NDPC

may be amended and expanded to provide for specific detailed regulations in sectors as diverse as:

a. Police and Security Data
b. Health data
c. Insurance data
d. Internet-specific data
e. Statistical Data
f. Financial Data
g. Social Security Data
h. Civil registration data
i. Direct Marketing data
j. Employment Data

2. **Expanding R(87)15 while overhauling CFD 977/2008/JHA** – The consolidation approach advocated in 1 above would be perfectly compatible with the clear need to further improve CFD 977/2008/JHA. While CFD 977/2008/JHA is strictly speaking the concern of the EU and not the Council of Europe or other states internationally, its primary functionality i.e. that of exchange across borders of personal data used for police purposes is one which is required by ALL member states of the Council of Europe and many of the world's states outside the confines of European territory. What is required and recommended here is that one of the Working Groups set up to implement Recommendation 1 above would be charged with the fusion and up-dating of two legal instruments: COE Recommendation R(87)15 on the use of personal Data for police purposes and CFD 977/2008/JHA in a way that it would respond to the requirements outlined inter alia by the EDPS i.e. to achieve real protection of the rights of data subjects within each member state and party to the NDPC rather than solely in exchange between states as currently provided for by CFD 977/2008/JHA. In this way, Police and Security issues would form one of the many sectors of application in which the NDPC would provide much more detailed guidance and protection.
    a. *Oversight* A further innovation by way of concrete measures in this instance could be the creation of internal Oversight functions at national and European- wide level charged with auditing the data protection standards applied by the police and security sectors in a way analogous to the Department of Justice OIG (Office of the Inspectorate General) oversight functions as introduced in the USA in relation to the FBI's use of National Security Letters.
    b. *Issues of adequacy and international reciprocity* – This category may immediately be organized into a number of initiatives which may be run in parallel but also in a way to ensure coherence with all the other measures indicated above and below. A prime example would be European-US issues. As indicated by the EDPS it does not make sense to have separate regimes for separate issues and an attempt should be made to resolve the following two areas in a way which is compatible with the rest of the NDPC's

"module" on personal data exchanged/accessed for uses by police and security: PNR Data and SWIFT Financial data.

3. Cyberspace and New technologies

a. Not all Cyberlaw deals with data protection law. Parts of Cyberlaw deal with e-commerce, others with cybercrime. Some of the new developments in cyberspace however, as already noted in Section 7 of the main report have a significant impact on privacy. These include the issues of explicit and informed consent as well as use of web-based activity to profile data subjects and the drafters of the NDPC would be well advised to address these, in addition to other priority areas like police and health care.

b. *Interventionism vs. individual choice* – A structured discussion of many of the above categories would possibly lead to a realization that clear decisions need to be taken about the desirability and indeed the necessity of governments to intervene in certain situations where key safeguards are currently being abused. Of particular importance to the drafting of the NDPC is the discussion on the notion of consent in data protection law and its situation in on-line practices. It is already clear that a good deal of processing of personal data is being undertaken without informed consent while explicit consent is being obtained through a "take it or leave it" attitude by on-line service providers. The de facto reliance of service providers on consent by their customers to use their personal data for a variety of purposes thus enables them to contract out of a number of basic protections, especially that of using data only for the purpose for which it was gathered. The way that things are currently set up, the data subject is often not well informed and the lack of real choice makes a travesty of the notion of informed and explicit consent as an effective safeguard. In the past, some national Governments have acted to "protect the citizen from himself" and in certain areas (e.g. genetic data) have explicitly prohibited the citizen from being able to contract his or her data protection rights away. There may be instances, especially in certain forms of on-line behavior such as social networking where such intervention may eventually prove to be advisable and necessary.

c. When considering the issue of consent and activity in Cyberspace, the Council of Europe would also be able to utilise the work of the TPD on the DRAFT RECOMMENDATION ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA IN THE FRAMEWORK OF PROFILING (see Appendix 8)

d. If the Council of Europe were to follow this recommendation and pursue Option 3, by the time that the relevant processes would be up and running, the Committee responsible for drafting the NDPC would also be able to benefit from some of the current research in this field. This includes EC-funded research on

   i. CONSENT in on-line social networking SSH 2009
   ii. SMART technologies in police, surveillance and security SEC 2010
   iii. Data protection in surveillance - SEC & SSH 2011

4. **An adequate debate on fundamental human rights issues such a *Lex Personalitatis* and Privacy.** When recommending Option 3, it is immediately apparent that this option may be pursued with or without an in-depth debate on fundamental human rights and privacy. There are strategic advantages and tactical disadvantages in having such a debate. Some may opine that the differences in the privacy law of the states invited to draft the NDPC would be so great that they would act as a distraction for and an obstacle to the NDPC ever getting off the ground. This may be a correct tactical judgement and this is why a careful reader would note that the proposal in these Recommendations is to have an NDPC and not necessarily a New Privacy & DPC (i.e. a NPDPC). This caveat made, it should be noted that the problems of the present lie chiefly in the past and many specifically arise because of the piecemeal way that European data protection law has come together since 1970. Thus, as a result, when, for example, tackling many of the subjects indicated in Recommendations 1-3 above, the participants involved in the drafting may be hampered by a relative lack of adequate inter-governmental debate on fundamental principles. In the past, the main premises of this debate have been largely side-stepped in spite of some valiant attempts to bring it up. Thus, when for example examining issues of data protection in Cyberspace, it would be normal for most EU policy makers to ask themselves the question: do we wish to formally create a right to on-line digital privacy as recently recognized by the German Constitutional Court? To do so it is necessary to re-open the debates commenced in the drafting of the Fundamental Charter of the EU especially those explicitly or implicitly on the rights of personality and informational self-determination. A mature European debate on these issues was stifled in the late 1990s by the obstructive or minimalistic approach taken by some national Governments. These Governments have since been replaced by others declaredly more sensitive to civil liberties and thus the time may now be right for a Council of Europe-led debate on the need to avoid a two-tier Europe in this field of privacy and data protection. Some may argue that the intransigence of some Governments in the past has already produced a two-tier Europe where a pack of roughly ten states led by Germany and including Denmark, Sweden, Norway, Romania, Hungary, Slovenia, Austria, have established privacy and data protection as being fundamental rights which are in themselves enabling rights which today serve to support the overarching right to free development of personality (*Lex Personalitatis*). It is this legal tradition developed over the course of 60 years which has enabled countries such as Germany to introduce the notion of informational self-determination and eventually the right to privacy on-line. It is respectfully submitted that a wide and open debate on this subject would enable it to be properly aired and give those Council of Europe member states as well as non-European states which are currently in the second tier (where such concepts are not yet articulated or rights embraced) the opportunity to choose for themselves as to whether they should be part of a fresh attempt to achieve international consensus in such matters. The recent debate in the European Parliament on the proposed accessibility to SWIFT data of the USA (January-February 2010) shows a strong interest in such matters by the elected representatives of EU citizens. Part of the package of measures that the Council of Europe may wish to consider is precisely that of a wide internal and external dialogue

on the subject of free development of personality and its links to privacy law, data protection law and other areas such as freedom of information. It is further submitted that this structured dialogue should not only be internal but also external and could be significantly enhanced by inviting all the members of the Committee drafting the NDPC to join the debate. This debate or structured dialogue may not necessarily result in consensus on every point but it may pave the way to a wider consensus on some issues which may then lead to benefits in many of the areas examined in the categories identified in this study. The debate may be held concurrently to the activities focused on the drafting of the NDPC rather than being formally part of it but it would be a significant contribution by the Council of Europe to our "understanding of WHY we are doing things".

5. **R & R awareness as a Policy option** – not all policy options for the Council of Europe need to be focused on legislative intervention. Indeed, European citizens may benefit greatly from a sustained awareness campaign intended to inform them of the **R**isks of information technologies to their privacy as well as the **R**emedies available to them to minimize risks and take all forms of remedial actions.

Concluding statement to Recommendations

Given the approach being recommended in these Recommendations, it is submitted that it is not appropriate for any specific wording to be prepared and especially not published before the first meeting of the Committee entrusted with drawing up the NDPC. That is where the dynamics of committee drafting come into play and where especially the Chairperson of that Committee would need to get a feel for the personalities and approaches of the delegates sent by the various participating countries. Moreover it is assumed that the Committee would include a number of experts with deep knowledge and long experience of Convention 108 and R(87)15. For it is the underlying principles of Convention 108 and R(87)15 and their ensuing logic which should be sacrosanct and not the wording. It should be recognized right at the very beginning of this "next phase process" that the procedure adopted to take Convention 108 and R(87)15 to their next stage of development within the NDPC is key to getting the right wording endorsed . The ideas and the specific wording must find their owners in every country participating in the process and this would help ensure a much more successful implementation of the new treaty when it is finally opened for signature. At this delicate stage therefore the recommendations made above were in the form of procedural and substantive guidelines for further action rather than specific proposals for the wording of a NDPC.

10/31/2010

Appendix Two

Data Protection Vision 2020

options for improving European policy and legislation during 2010-2020

Joseph A. Cannataci

The application of information technology has engendered a dilemma. On the one hand, technology has made it possible to monitor and supervise various forms of activities: the protection of the public being the prime concern. On the other hand, the very possibilities offered by information technology pose a threat to our social wellbeing: our privacy is endangered, and new means for fraudulent behaviour and other forms of anti-social behaviour have been created. While monitoring and supervision may alleviate certain problems, it may in itself create new problems.

In 2006, the Centre for Computers and Law of the Erasmus University Rotterdam, the Netherlands, hosted a Workshop on the subject of Monitoring and Supervision. The Workshop was organised in close cooperation with LEFIS, the Legal Framework for the Information Society, and with the Dutch Research School for Safety and Security in Society. This report contains a selection of papers presented during this workshop and concludes with a number of observations by the editors.

P. Kleve, R.V. De Mulder & C. van Noortwijk (Eds.)

Monitoring, Supervision and Information Technology

Monitoring, Supervision and Information Technology

Proceedings of the first international seminar of the Legal Framework for the Information Society (LEFIS) on Monitoring, Supervision and Information Technology

15 June 2006

Editors:
P. Kleve
R.V. De Mulder
C. van Noortwijk

Centre for Computers

Monitoring, Supervision and Information Technology

Proceedings of the first international seminar of the Legal Framework for the Information Society (LEFIS) on Monitoring, Supervision and Information Technology

15 June 2006

Erasmus University Rotterdam
The Netherlands

Editors:
P. Kleve
R.V. De Mulder
C. van Noortwijk

2006

Legal Framework for the Information Society (LEFIS)

Research School for Safety and Security (OMV), Erasmus University Rotterdam

Centre for Computers and Law, Erasmus University Rotterdam

ISBN 905677316X

Table of Contents

consensus on what is a good parental style. Similarly, in the case of supervising and monitoring children's activities on the Internet, there is no clear indication of how parents should supervise their children's activities. Though there are debates and suggestions that parents should use filtering software, such suggestions for me come with economical burden. Not every parent can afford to buy filtering software, although, in some circumstances, the software can be downloaded from the Internet be it with limited efficiency. Subscribing to firewalls or filtering software from the Internet Service Providers (ISPs) sometimes has a high price tag too, so parents prefer to provide the facilities of a computer and Internet first before thinking about the safety aspects.

4. Discussions and Conclusions

To make parents responsible for the adverse effects of the Internet to children *per se* is not fair as we need to examine external factors which may influence the upbringing of children. Many adults need help in learning how to grow with their children as ICT advances. Some need education and guidance from professionals in order to function as competent parents. However, the notion to totally blame or punish the parents for their child misdeed or crime needs to be placed with caution. Fortin argues that government intervention in family life between all parents and children through legislation has traditionally provoked strong hostility especially if such legislation threatens to interfere with the parent-child relationship.[25] The responsibility to protect children from risks should not be on parents alone, society must also protect children from risks. However, risks on the Internet are difficult to assume due to the very nature of the Internet. Hence, the state and the ISPs play a crucial role in educating parents on safety on the Internet. Before parents subscribe to the Internet, they should be informed by ISPs on the dark side of using the Internet that may affect them and their children. Without a reminder from the ISPs to keep an eye on child safety, parents will overlook the need to supervise their children's activities. It is possible to punish parents if it is proven that parents have negligently failed to take precautionary steps to ensure that their children's activities on the Internet are in line with the nature of children who need protection and guidance from parents from time to time. Parenthood itself should not be seen as burden but it is a developmental stage in the life cycle. Parenthood itself needs the support from state and society at large. Westman states that the maturing and emotionally satisfying elements of parenthood are fundamental, if not explicit, motivations to become parents.[26] The support given will definitely be cherished by today's modern parents in facing the challenges in bringing up children in an age of technology. I believe that the notion of punishing parents for child's misdeeds on the Internet is a reminder to negligent parents to take their duties seriously.

[25] Fortin, J. (2003) *Children's Rights and the Developing Law*, 2nd Ed UK, LexisNexis Butterworths, p8

[26] C. Westman, J. (1999) Children's Rights, Parents' Prerogatives and Society's Obligations. *Child Psychiatry and Human Development.* Vol 29(4), Summer, p 327.

R (87) 15: A Slow death?

Joseph A. Cannataci, Mireille M. Caruana, Jeanne Pia Mifsud Bonnici[1]

Abstract

Recommendation R (87) 15 was vaunted as being possibly one of the most successful products of the Council of Europe's Committee of Experts on Data Protection. Its adoption as an Annex to the Schengen Agreement meant that it became (or was expected to become) the de facto data protection standard for police forces across Europe.

Nearly twenty years have passed since R (87) 15 was finalised in the teeth of much opposition from a number of security forces across Europe. The methods chosen by terrorists and criminals since 1987 have also taken a number of new directions making police and security forces even hungrier users of personal data. On the face of it, in spite of three review exercises, R (87) 15 has been retained intact. Indeed by 1992 (in Recommendation 1181(1992)1 on police co-operation and protection of personal data in the police sector) the member states of the Council of Europe had agreed to move towards a convention enshrining the principles of R (87)15. Fifteen years from R 1181(1992)1, R (87)15 has never made it to convention status. The data protection star is on the wane and, while some continue to pay lip service to R(87)15, a number of measures have been agreed at the European level which appear to undermine the spirit if not the letter of the landmark recommendation which is so unloved by police forces.

This paper traces the review processes of R (87) 15 within the Council of Europe and the up-grade measures considered within the CJ-PD (Committee of Experts on Data Protection). These are then contrasted with actual developments which resulted in the recommendations of the Working Party on Data Retention and the resultant ignoring of the data protection position by the Council of Ministers and Parliament. New technologies like biometric passports have led to agreement at the European level which further promise widespread collection of personal data by police and security forces. These recent developments fuelled by concerns rendered more acute in the wake of 9/11 may be interpreted as signifying the beginning of the end for R (87) 15 or alternatively as being merely part of the downward graph in a cyclical evolution of a data protection culture.

[1] Professor Joseph A. Cannataci is Head of the Lancashire Law School at the University of Central Lancashire UK. Dr. Mireille M. Caruana is a Visiting Lecturer at the University of Malta. Dr. Jeanne Mifsud Bonnici is a Research Fellow at the Centre for Law & IT at the University of Groningen, The Netherlands.

"My anxiety is that we don't sleepwalk into a surveillance society where much more information is collected about people, accessible to far more people shared across many more boundaries than (British) society would feel comfortable with..."

(Richard Thomas – August 2006)

1. Introduction

Many newcomers to the field of data protection law, at first, fail to notice that the crux of most arguments boils down to "purpose" or, as the French would call it, *"finalité"*. What is the purpose for which the personal data is being collected in the first place and what is the onward-use of such data? Is it compatible with the purpose for which the data was collected in the first place?

This is the fundamental tension underlying use of certain personal data by police and security forces and it revolves around a central tenet of data protection law i.e. that personal data can only be processed for the purpose(s) for which it was collected. This is a principle inimical to the basic instincts of many police officers in what they often view as being their sometimes unequal war on crime. Police officers often wish to use personal data irrespective of the purpose for which it was given: what they view as important is "does it provide a lead? Does it help detect or prevent an offence?". If that is the case, then purpose can take a second seat to the security of society and/or the prevention of crime.

This tension is not something new. It has existed from the very beginning, from the very first attempts of applying basic data protection principles to the police and security sectors. Indeed, it arises out of, or is at least related to, a tension that pre-dates classic data protection laws. Privacy and security have never been easy bedfellows. Numerous attempts at keeping police forces in check within a democratic society (e.g. interception of telecommunications) have always striven hard (and sometimes failed) to strike the right balance between the individual's right to privacy and the public's (in this case the police's) right to know.

Nor is it solely police use of personal data that raises problems of underlying tensions with the fundamental principle of purpose that underpins all of European data protection law. The UK Information Commissioner, Richard Thomas, recently summed up his concerns in the following manner:

"Some of my counterparts in Eastern Europe, in Spain, have experienced in the last century what can happen when government gets too powerful and has too much information on citizens. When everyone knows everything about everybody else and the Government has got massive files, whether manual or computerised..."

"I don't think people have woken up to what lies behind this. It enables the Government of the day to build up quite a comprehensive picture about many of your activities. My job is to make sure no more information is collected than necessary for any particular purpose."

Thus although Thomas does not oppose the idea of identity cards, insisting that he cannot be *"for or against"*, he is critical of the UK Government's failure to spell out in a draft Bill the cards' exact purpose. He says:

"The Government has changed its line over the last two or three years as to what the card is intended for. You have to have clarity. Is it for the fight against terrorism? Is it to promote immigration control? Is it to provide access to public benefit and services? Various other reasons have been put forward... I don't think that is acceptable."[2]

In this interview, Richard Thomas is questioning the precise purpose of proposed ID cards in the UK and asking as to whether the fight against terrorism is the main purpose for having personal data collected and stored in order to issue UK citizens with an ID card. Thomas appears to be here still fighting for the basic tenet of purpose, but this paper asks whether this battle has already been lost, at least insofar as use of personal data by the police is concerned. It is crucial, at this stage, to also determine certain perspectives: are laws and fundamental principles so absolute that, once recognized, they can exist inviolate or are they cyclical in their appreciation, development and consolidation? Are certain principles in data protection law rather like trees and plants that are laid bare by the winter but return in full bloom by the spring and the summer before moving again into the less clement cycles of autumn and winter...only to flourish again once the climate is favourable in the next part of a perpetual cycle? Or are such perspectives merely wishful thinking on the part of privacy advocates who refuse to countenance the fact that some rights have been irretrievably lost?

Thinking about cycles and taking the long view of the history of legislation is a salutary exercise for, clearly, the fragility of man's respect for fundamental human rights may be measured by the relative youth of such concepts in legal

[2] In an interview with The Times available at http://www.timesonline.co.uk/newspaper/0%2C%2C2710-1218615%2C00.html as reported on the 16th August 2006

history. It took the best part of four thousand years from the Codex of Ur-Nammu[3] and the more famous one by Hammurabi[4] for society to come up with the 1948 United Nations Declaration of Human Rights,[5] the first international instrument to recognize a right to privacy.[6] Article XII states that "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."

Then again some would argue that this advance from a system of law that was largely property-based[7] to one that recognizes rights pertaining to human beings, their personality and their dignity, wherever they may be and whatever their ethnic origin or religious belief, had to be jolted along by the carnage wrought by two world wars. The internationalization of war on such a massive scale as seen during the twentieth century, coupled with the ubiquity of media and information technologies, has led to an almost proportionate internationalization of law, and privacy is no exception.

The space available in this paper does not afford a full-scale debate on the notion of cycles in history or in legislative history in particular, yet "the recent development of mathematical models of long-term ("secular") socio-demographic cycles has revived interest in cyclical theories of history ".[8] It is tempting to view the past and current developments of data protection law as part of an historical cycle, though where the cycle will lead to next is difficult to predict since privacy is such a relatively new area of law.

Such patterns and cycles, including legal development at the national level[9] and subsequent spread to the international level have long been discernible in privacy law, as have been the links to various forms of information technology. The printing press was the technology that communicated and amplified the thinking of the French *philosophes* and underpinned a lot of what happened at the national level during the French Revolution of 1789. Yet, the same

3 Ca 2050 BC

4 Ca 1780 BC

5 Adopted and proclaimed by the UN General Assembly on 10 December 1948.

6 See Article XII.

7 Hammurabi's code focussed chiefly on focuses on theft, agriculture (or shepherding), property damage, women's rights, marriage rights, children's rights, slave rights, in addition to more fundamental issues such as murder, death, and injury

8 http://en.wikipedia.org/wiki/Philosophy_of_history. See, for example, Peter Turchin, Historical Dynamics: Why States rise and Fall, (2003) Princeton University Press, for an American take on macromodels and the even more recent Andrey Korotayev et al. Introduction to Social Macrodynamics (2006) Moscow, URSS for a Russian but not altogether dissimilar line .For a different approach to historical cycles see William McGaughey, Five Epochs of Civilization (2000) Minneapolis: Thistlerose Publications .

9 Although even the term "national development" is suspect in an area where thinking is growingly international, since the exchange and influence of ideas across national boundaries is already well apparent at the time of the US Declaration of Human Rights and the French Revolution.

technology also contributed enormously [10] to the birth of a new nation even before the French revolution, as may be seen, say, in the impact of the articles and pamphlets of Thomas Paine in the period leading to the American Declaration of Independence of 1776. Between 1789 and 1791 the Bill of Rights, comprising the first ten amendments to the United States Constitution, was adopted. All ten amendments relate to limiting the power of the federal government. The Fourth Amendment in particular guards against searches, arrests and seizures of property without a specific warrant or a "probable cause" to believe a crime has been committed. A general right to privacy has been inferred from this amendment and others by the Supreme Court of the United States[11], although it remains to be said that the line of cases deriving there from remains controversial and has drawn accusations of judicial activism.

It took over another 150 years for some of the principles established and developed within the First Amendment of the United States constitution to become sufficiently internationalized at the UN and European level. A couple of years before the European Convention of Human Rights of 1950[12] upheld a general right to privacy[13], in 1948 George Orwell was writing "Nineteen Eighty-Four". The nightmare fantasies depicted by George Orwell in this classic work of fiction did not even contemplate the existence of what was to come – the pervasiveness of computers and the invention of the World Wide Web. Yet they were part of an important cycle, as the Europe of the dictators that preceded World War Two came together to reject the past, the spectre of totalitarianism that was to cast a sinister shadow over the whole of the Cold War. 1989 saw the beginning of the end of what historians may eventually call the "Soviet cycle of totalitarianism". 1989 led to 15 years of optimistic growth with a European Economic Community that became a Union which went from 9 to 25 members by 2004 and a Council of Europe that, during the same period, went from 21 members to 46.

If the misery of the two world wars led to the birth of the welfare state and the prosperity of the 1960's, the death of the European colonial empires and the battle of ideologies led to the cycles of terrorism that afflicted France, Germany and Italy in the 'sixties and the 'seventies. The industrial unrest of the 'seventies and early 'eighties also witnessed the crushing of the Baader-Meinhof gang in Germany and the Brigate Rosse in Italy, and once again gave way to the prosperity and optimism of the late 'eighties and early nineties. Could anyone be blamed for seeing up-beat privacy legislation at the national and European levels

10 See for example the impact of the various publications as evidenced in Gertrude Himmelfarb, The Roads to Modernity: The British, French and American Enlightenments, (2004) and especially in this example, the writings of Thomas Paine as summarised in http://en.wikipedia.org/wiki/Thomas_Paine

11 See Griswold v. Connecticut, 381 U.S. 479 (1965), a landmark case in which the Supreme Court ruled that the Constitution protected a right to privacy.

12 Signed in Rome on 4 November 1950, available at http://conventions.coe.int/treaty/en/Treaties/Html/005.htm

13 Article 8; Article 10 of the same Convention guarantees the right to freedom of expression.

in the latter half of the eighties and the first half of the nineties? Convinced that the values of the liberal West had triumphed, it was perhaps only natural that the years 1986-1996 were characterized by an apparent entrenchment of the data protection principle of purpose specification in many levels.

This entrenchment had been a long time in the making: the privacy debate in the US between 1966 and 1973 which led to the Federal Privacy Act 1974 had made its way across the Atlantic and, following two resolutions of the Parliamentary Assembly in 1974 led to the birth of the Council of Europe's Committee of Experts on Data Protection in 1976. Yet another five years of international haggling led to the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[14] (hereinafter referred to as Convention 108) and almost another 5 years for this Convention to come into force in 1985. Spurred on by visions of "1984" and with totalitarianism in the East still apparently very much in the driving seat, the years 1984-1986 were taken up by intensive debate which, in 1987, saw agreement being reached upon Recommendation No. R (87) 15 regulating the use of personal data in the police sector (hereinafter referred to as R (87) 15).

1995 saw the European Union twist the arm of (at least some of) its member states to enact harmonized national legislation on data protection when it passed Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter referred to as Directive 95/46)[15], which all EU member states were required to implement into national legislation by 24 October 1998. The Schengen Agreement also came into effect in 1995, including a reference to R (87) 15.

It will be seen that the 1986-1996 period of consolidation in data protection law gave way to another dip in the cycle. Directive 95/46 had barely come into effect in 1998 when concern with data privacy was heavily off-set by security concerns, especially following certain specific events. 2001 saw the great tragedy widely and simply referred to nowadays as "9/11". Terror struck the USA in an unexpected and phenomenal manner. Exactly 912 days after the 11th September terrorist attack on America in 2001, terror also struck in Europe when on the 11th March 2004 a series of coordinated bombings against the commuter train system of Madrid, Spain, killed 192 people and wounded 2,050. The next successful attacks in Europe were the London bombings which occurred in July, 2005.

The tension between two fundamental societal values is immediately evident: on the one hand, the right of the citizens to be protected from terrorism and the obligations of a sovereign State to fight against it and safeguard public security,

[14] Strasbourg, 28.I.1981; Available at http://conventions.coe.int/Treaty/EN/Treaties/Html/108.htm
[15] Official Journal L 281, 23/11/1995 P. 0031 – 0050, available at http://europa.eu.int/comm/internal_market/privacy/law_en.htm

and on the other hand, the individual's right to personal data protection and privacy. With the declared aim of providing a vital tool against terrorism and serious crime in the hands of the law enforcement agencies across Europe, 2006 saw the finalization of the Data Retention Directive.[16]

R (87) 15 has, despite opposition, remained unchanged since its introduction in 1987. But are we in Europe in fact "killing [it] softly", as it begins to pass unobserved and legislation purportedly infringing on civil rights and in violation of the spirit, if not also of the word, of the said Recommendation is passed as if it were a simple matter of course? Before proceeding to see where this part of data protection law fits within successive cycles of domestic and international terrorism, it is worth examining its birth and development in some further detail.

2. The painful birth of R(87) 15

Fourteen months before Mr. Gorbachev had his fateful meeting with Mr. Bush in Malta but scarcely three years after the unsuccessful IRA attempt to blow up Margaret Thatcher, on the 17 September 1987 the Committee of Ministers adopted Recommendation No. R (87) 15 regulating the use of personal data in the police sector. This Recommendation (hereinafter referred to as R (87) 15) was a victory for the basic principle of data protection of "purpose specification".[17] Principle 2 of R (87) 15 provides 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. Any exception to this provision should be the subject of specific national legislation"* and later further provides that *"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. The collection of data concerning these factors may only be carried out if absolutely necessary for the purposes of a particular inquiry."*

Principle 2.3 of R (87) 15 provides that "*The collection of data by technical surveillance or other automated means should be provided for in specific provisions.*"

Principle 3.1 of R (87) 15 provides that "*As far as possible, the storage of personal data for police purposes should be limited to accurate data and to such data as are necessary to allow police bodies to perform their lawful tasks within the framework of national law and their obligations arising from international law.*"

[16] Directive 2006/24/EC
[17] Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data. Strasbourg, 28.I.1981 – in particular, Article 5.

These three key principles of R (87) 15 were not easily won. The Recommendation was born within the Council of Europe's Committee of Experts on Data Protection (CJ-PD) in Strasbourg during the years 1984-1986. CJ-PD was characterised by the strong leadership of Germany's Spiros Simitis, later involved in including data protection in the EU Charter of Fundamental Rights, and succeeded by Peter Hustinx, today EU Data Protection Commissioner. Many of the data protection experts at CJ-PD were accompanied by representatives of the police and security forces of their countries. The representatives of the police and security forces were asking for "general purpose" collection, as opposed to the position of the CJ-PD (as also of Convention 108) enlisting "purpose specification" as a basic principle of data protection. It was only as a result of very strenuous negotiations that it was possible to arrive at a consensus basis for the eventual text. The Police and security officials involved could draw upon the very recent memories of the Baader-Menihof and the Brigate Rosse campaigns in Germany and Italy not to mention the on-going campaigns of the IRA in mainland Britain[18] and their interventions before, during and after CJ-PD meetings were intended to minimise the effect of any eventual recommendation on Police operations but, on this occasion at least, they had to bow to the strength of the data protection lobby.

This was especially so when dealing with purpose specification. Convention 108 had created ambiguity by allowing an exclusion from its provisions for security purposes.[19] R (87)15 resolved this ambiguity by unambiguously subjecting police data to the same data protection regime as other data. R(87)15 thus scored a victory by entrenching the notion of purpose for collection and processing of data, even for police use.

[18] Though the mid-1980s saw a lull in IRA bombings in Britain until they commenced again in the early nineties.

[19] Article 9.

3. In the ascendant: the early years 1987 – 1993

R (87) 15 was never popular with the police in Western Europe, although it was greeted as a model for democracy and cited often, especially in the 1989-1992 period, in Central and Eastern Europe.[20] In the face of R(87)15 and then Directive 46/95, Police forces had to at least pay lip service to the principles of data protection.[21]

In the post-1989 surge forward for democracy, R (87) 15 was adopted as the data protection standard for the Schengen Treaty. In order to reconcile freedom and security in the Schengen area, freedom of movement was accompanied by so-called "compensatory" measures. This involved improving coordination between the police, customs and the judiciary and taking necessary measures to combat important problems such as terrorism and organised crime. In order to make this possible, an information system known as the Schengen Information System (SIS) was set up to exchange data on people's identities and descriptions of objects which are either stolen or lost.

In 2001 Switzerland was given the authority to negotiate for accession to the Schengen Convention. The Office of the Federal Data Protection and Information Commissioner then stressed, *inter alia*, that the problems connected with Switzerland's accession should not be seen as a weakening of data protection resulting from Switzerland's participation in an international system of co-operation. On the contrary, Switzerland's accession would in fact benefit data protection by imposing a clearly defined and delineated framework around the data processing operations required for the exchange of information with the contractual parties. This would ensure that standards are demanding and in conformity with the standard of European data protection legislation.

[20] An outstanding example of how security forces may indiscriminately collect data and, through the control of that information, control the society in which they operate is that of the Ministerium für Staatssicherheit (MfS / Ministry for State Security), commonly known as the Stasi, the main security (secret police) and intelligence organisation of the German Democratic Republic (East Germany). The Stasi amassed incredible amounts of data collected by all sorts of illegal and secretive means and was widely regarded as one of the most effective intelligence agencies in the world. Its influence over almost every aspect of life in the German Democratic Republic cannot be overestimated. Until the mid-1980s, a civilian network of informants called Inoffizielle Mitarbeiter grew within both East and West Germany. It is estimated that approximately one in fifty East Germans collaborated with the Stasi – one of the highest penetrations of any society by an intelligence gathering organization. During the 1989 peaceful revolution, the Stasi offices were overrun by enraged citizens, but not before a huge amount of compromising material was destroyed by Stasi officers. The remaining files are available for review to all people who were reported upon, often revealing that friends, colleagues, husbands, wives and other family members were regularly filing reports with the Stasi – a picture of a truly Orwellian society.

[21] There is disturbing anecdotal evidence (but no hard evidence as yet uncovered) that the respect of R(87)15 was patchy at best, with some forces in Europe trying to stick to the letter and spirit of the recommendation and others far more openly flaunting the rules on "purpose", remaining very happy to get hold of "interesting" personal data, never mind when it came from. Informal contacts between officers in different national forces appear to very often bypass any controls on personal data export across borders.

Switzerland's accession - *in particular on account of the strict limits imposed on the purposes and uses of the data* - would create a better set of conditions for flows of information and would thus provide better guarantees for the persons affected.[22]

On the face of it, there was no stopping R (87) 15 in the early years. In its **Recommendation 1181 (1992)1 on police co-operation and protection of personal data in the police sector**, the Parliamentary Assembly of the Council of Europe, recommended that the Committee of Ministers, among other things, draw up a convention enshrining the principles laid down in R (87) 15. It was noted that as a result of the Schengen Agreement, the European states co-operating in that agreement will proceed with the exchange of automatically processed personal data in the police sector. At that time, there was already an intensive exchange of data in the police sector among Council of Europe member states on a bilateral or multilateral basis and through Interpol. It was considered to be of vital importance for an efficient combat against international crime that it is fought at national and at European level. Moreover, an efficient fight against crime implies an exchange of data in the police sector. In this respect, it was considered useful to recall the Assembly's Recommendation 1044 (1986) on international crime and its plea for a European information and intelligence centre (Europol), and Recommendation No. R (87) 15 of the Committee of Ministers to member states of the Council of Europe regulating the use of personal data in the police sector. It was considered necessary, however, that there be adequate protection of personal data in the police sector. The Parliamentary Assembly therefore recommended that the Committee of Ministers:

i. draw up a convention enshrining the principles laid down in its Recommendation No. R (87) 15 ;
ii. promote the application of these principles in the exchange of data in the police sector between member states and between member states and third countries via Interpol.

[22] The Schengen Convention from the Viewpoint of Data Protection (July 2002) – Available at http://www.edoeb.admin.ch/dokumentation/00445/00509/00513/00765/index.html?lang=en

4. The first skirmish: 1993

In 1993 the Project Group on Data Protection (CJ-PD) was requested by the Committee of Ministers of the Council of Europe to evaluate the relevance of R (87) 15 and in particular the need to revise the text, namely its scope and principle 5.4 (international communication), bearing in mind the principles set out in Assembly Recommendation 1181 (1992). The Project Group reached the conclusion that R (87) 15 gave adequate protection for personal data used for police purposes and that, at that stage, there was no need to revise it, or parts of it. The Project Group felt that Article 5.4 of R (87) 15, especially when read together with paragraphs 56-80 of the Explanatory Memorandum, appeared flexible enough to meet the foreseeable requirements of international agreements on the exchanges of data for police purposes.

In preparing for these conclusions, the Rapporteur[23] of the Group performed a qualitative analysis on all the national reports of the member states submitted. He reported that the response overview reinforced the impression that R 87 (15) continued to provide a sound basis for data protection in the police sector. The text of R 87 (15) was considered to be sufficiently elastic to permit the various interpretations that some member States may have wished to see specifically mentioned in the text or, more often, in the Explanatory Memorandum. This very fact would militate more in favour of maintenance of the current text rather than the re-opening of the Pandora's box that re-formulation of the text could have brought about. Moreover, several experts concurred "that the provisions of the Recommendation constitute an inalterable necessary minimum" (CJ-PD (93) 48). The number of requests for serious revision of the text, whether to strengthen or to weaken the provisions, was deemed to be too small to merit a re-opening of the discussion on R (87) 15 as a priority matter for the Project Group on Data Protection. With regard to the specific relevance of Article 5.4, it was considered that no overwhelming arguments had been advanced as to why the formulation of Principle 5 (Communication of data) and its accompanying Explanatory Memorandum failed in providing the most balanced formula capable of providing equitable provision for current requirements.

Finally, the Project Group nevertheless proposed that the relevance of R (87) 15 should become the subject of periodic review on a regular rather than an ad hoc basis. For this purpose, it further proposed that the next review be carried out and reported on by December 1998 and thereafter on a four-yearly basis.

[23] The 1993 Rapporteur to the CJ-PD was J.A. Cannataci, one of the co-authors of this present study.

rivacy 1996-2001

gns of a losing battle could
he concern with cyber-crime
h privacy. Despite the long-
developing data protection
h of privacy as a substantive
role of the US in the drafting
mable – in order to get the US
mittee of Experts on Crime in
Privacy as an issue. When
JS was mostly interested in
ting a 24/7 Network for
or proceedings concerning
s and data and creating a
nd subsequent prosecution.
justice experts wanted to be

r of other successes under its
Medical Data,[24] a second on
ommendation: the Guidelines
priority work, the CJ-PD did
of R(87)15 and indeed, the
ost respected members, Mr.
Justice. The 1998 Report by
ce of Recommendation No. R
police sector – thus followed
d was concurrent with the on-
Crime Convention. The 1998
oblems had been raised that
dation. The report proposed
national legislators explicitly
either in the national Data
edure, or national or regional

e powers, to be adequate,
life and should therefore be

restricted to the extent that is necessary. It was proposed that the Committee of Ministers of the Council of Europe change their original decision to evaluate the 1987 Recommendation periodically in the sense that periodically the question be answered whether any *additional international instrument* should be developed. The integrity of R (87)15 was thus preserved in this second mini-sub-cycle within a three cycle review process.

7. The third report: 2002

The report on the third evaluation of R (87) 15 was completed in 2002. The CJ-PD examined Recommendation R (87) 15 and agreed that "its principles are still relevant, continue to provide a basis for the elaboration of regulations on this issue and serve as a point of reference for any activities in this field and considered that it is not necessary to revise them at present. Furthermore, this Recommendation is referred to in other international instruments such as the Schengen Agreement and the Europol Convention". Therefore, CJ-PD would not recommend any revision of Recommendation No. R (87) 15 or the preparation of a new recommendation in the police field. The Report also recommended that the third evaluation should be the last of the periodic evaluations and that since the use of personal data in the police sector remains a continuing concern, where necessary further evaluations of specific issues arising in relation to the development of new techniques of processing police data could be carried out. Is the tone of the final evaluation an attempt at casting R(87)15 in stone in face of an increasingly hostile world?

8. Killing R (87) 15 Softly?

In the first evaluation report of R (87) 15 the Rapporteur quoted the stance typically expressed in the strongest terms by the Swiss Federal Data Protection Officer who "takes the view that these Regulations should not be weakened under any circumstances and that the principles set out in Recommendation R (87) 15 should be regarded as established". The CJ-PD appears to have remained consistent with this view over all three re-evaluation exercises but is this enough? Are we in fact killing R (87) 15 softly because while it was ultimately never revised, in whole or in part, other regulations and practices are in fact emerging that undermine the protection given by R (87) 15 for personal data used for police purposes?

9. Changing times – 9/11 – PNR data ....is the May 2006 ECJ decision a 'small' victory?

Terrorism presents our society with a real and pressing challenge. Governments must however respond to this challenge in a way that effectively meets their citizens need to live in peace and security while not undermining their fundamental human rights – including the right to data privacy – which are a cornerstone of our democratic society.

R (87) 15 was created when Europe had largely settled the terrorist issues which had plagued Germany and Italy in the '70s, though the IRA problem was far from solved for the British, the Belgians were in the grip of a terror rampage of their own while the Gladio scandal[27] had yet to explode fully in Italy. Yet, by the end of the 20th Century, while terrorism had become very common-place, almost part of daily life in Europe, this was not the case in the United States. 2001 brought with it 9/11 – a disaster which heralded much trouble for data protection. The first victim was the airline passenger lists resulting in a dispute between the EU and the US.

Following the terrorist attacks of 9/11, the United States passed legislation providing that air carriers operating flights to, from or across US territory have to provide the US authorities with electronic access to the data contained in their reservation and departure control systems, called 'Passenger Name Records' (PNR).

The Commission adopted, on 14 May 2004, a decision[28] finding that the United States Bureau of Customs and Border Protection (CBP) ensures an adequate level of protection for PNR data transferred from the Community. On 17 May, 2004 the Council adopted a decision[29] approving the conclusion of an agreement between the EU and the United States on the processing and transfer of passenger name records (PNR) data by air carriers established in the EU member states to the US customs and border protection. The agreement was signed on 28 May 2004 and entered into force right away.

[27] The Gladio scandal was the first official confirmation by a Head of Government that NATO has a secret plan of "stay-behind armies"...accompanied by many accusations that these "security forces" had actually run amok in some Nato countries, actually carrying out anti-democratic actions and even terrorist attacks. For a fuller account of this version of history, see Daniele Ganser, NATO's Secret Armies, Operation Gladio and Terrorism in Western Europe (2004) Zurich.

[28] Commission Decision 2004/535/EC of 14 May 2004 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States Bureau of Customs and Border Protection (OJ 2004 L 235, p.11).

[29] Council Decision 2004/496/EC of 17 May 2004 on the conclusion of an Agreement between the European Community and the United States Department of Homeland Security, Bureau of Customs and Border Protection (OJ 2004 L 183, and corrigendum at OJ 2005 L 255, p.168).

In September 2004, the European Parliament brought a legal case against the Commission in the European Court of Justice (ECJ) on the EU/US passenger name records (PNR) agreement. Parliament accused the Commission of misuse of powers, breach of fundamental rights and of the principle of proportionality. The Parliament also appealed to the ECJ for annulment of the Council decision adopting the agreement. The European Data Protection Supervisor intervened in support of the Parliament in both cases, the first intervention before the Court by that authority since its establishment.

On 30 May 2006 the European Court of Justice ruled that *"neither the Commission decision finding that the data are adequately protected by the United States nor the Council decision approving the conclusion of an agreement on their transfer to that country are founded on an appropriate legal basis"*. The ECJ judgment thus annulled both the Commission and Council decisions on a technicality which did not address the substantive issues. The agreement as such was not annulled.

With regard to the Commission decision on adequacy, the Court held that in view of the fact that the first indent of Article 3(2) of Directive 95/46 excludes from the Directive's scope the processing of personal data in the course of an activity which falls outside the scope of Community law, such as activities provided for by Titles V and VI of the Treaty on European Union, and in any case processing operations concerning public security, defence, State security and the activities of the State in areas of criminal law, and also in view of the fact that the transfer of PNR data to the CBP constitutes processing operations concerning public security and the activities of the State in areas of criminal law, the said decision on adequacy did not fall within the scope of the Directive. Therefore, the Court annulled the decision on adequacy and held that it is not necessary to consider the other limbs of the first plea or the other pleas relied upon by the Parliament.

With regard to Council Decision 2004/ 496, the Court held that the Agreement relates to the same transfer of data as the decision on adequacy and therefore to data processing operations which are excluded from the scope of the Directive. The Court therefore also annulled the said Council Decision on the ground that it couldn't have been validly adopted on the basis of Article 95 EC as Article 95 EC, read in conjunction with Article 25 of the Directive, couldn't justify Community competence to conclude the Agreement. Once again, the Court held that it is not necessary to consider the other pleas relied upon by the Parliament.

Data transfers continued during a transition period until 30 September 2006, after which the ECJ judgment was to take effect. But the Commission quickly acted to remedy the situation in favour of data transfers: by the 6th October 2006 the United States and the European Union established a temporary arrangement for the transfer of personal information on European travellers that will expire in

July of 2007. The new agreement gives the Europeans greater control over the disclosure of passenger data to the United States. However, it leaves unresolved whether the United States has adequate privacy protections to safeguard the private information of European consumers.[30]

On balance, the decision of the ECJ cannot be considered to be much of a victory for the data protection lobby. On the contrary, as Peter Hustinx, EDPS, points out: "The judgment seems to have created a loophole in the protection of European citizens whereby their data are used for law enforcements purposes. This makes it all the more important that a comprehensive and consistent legal instrument ensuring the protection of personal data outside of the first pillar is adopted without delay".

This comment by Hustinx is especially interesting. The reference to first pillar is intelligible only in an EU context where security and crime prevention did not fall within the scope of the original EU treaty. Yet, most of the major players in the EU are also signatories of Convention 108, wearing their hats as member states of the Council of Europe, which is further amplified in R(87)15. So, while matters between the EU and the US may be currently falling into some form of legal limbo, at the level of individuals, anybody appealing to the European Court of Human Rights in Strasbourg (as opposed to the ECJ in Luxembourg) would be likely to have a court that will take both Convention 108 and R(87)15 into account.

To get to the Strasbourg Court however, an individual must exhaust all local remedies and the current frame of mind in European legislators across Europe is possibly making this more difficult. The recent case of Hungary perhaps illustrates this point best. On the 29th November 2006, the Hungarian President Laszlo Solyom returned to the Parliament the bill about the promulgation of the agreement on registration of travellers' data concluded between the European Union and the United States of America.

The Hungarian President Laszlo Solyom decided not to sign the national law regarding the promulgation of the EU-US PNR (Passenger Name Records) agreement and sent it back to the Parliament, considering that it can be improved. It has been claimed that "This is one of the few set-backs of the new EU-US PNR agreement concluded in October 2006, even though there have been numerous critics to the content of the new agreement that makes possible for air companies to send to US authorities the personal data of the passengers that were registered in the booking system".[31]

[30] It is only the Department of Homeland Security which is considered to offer adequacy in this agreement

[31] http://wwwkeh.hu/keh_en/news/20061129communique.html and http://www.tasz.hu/index.php?op=contentlist2&catalog_id=3496

According to the Hungarian President "it is necessary that the Parliament make possible the forwarding of data in the act on promulgation of the international agreement only in case the person in question has explicitly approved of it. The President's opinion is that a regulation of such content would not be contradictory to the international agreement."

Therefore, Mr. Solyom asked the Parliament to re-discuss the bill and to complete it with a rule that stipulates for the explicit approval of the person in question to forward of his data abroad. However laudable the intentions of the Hungarian President may be, it is difficult to see how effective a protection of privacy this can be since most passengers will be compelled to give their explicit consent since they do not have much choice in the matter...unless they give their consent they won't get their air ticket![32] In other words, the protection offered by R(87)15, explicit consent of the data subject will not be worth much in real terms, the situation will be provided for by domestic law and the data subject will have no basis for appeal to the Strasbourg court.

As ever, there may be other issues which colour this cycle of developments: "The (Hungarian) Government might not push too much this issue since the U.S. President
promised last week that he will ask the Congress to waive the visa obligations of the new EU member states. Dr. Kinga Göncz, the Minister of Foreign Affairs was asked by journalists if the President's action could jeopardise Hungary's chances in obtaining a visa free status from the U.S. The minister replied she hopes the problem will be solved soon as it might cause problems in the long run."[33]

[32] Adam Foldes, the Data Protection Program Director within the the Hungarian Civil Liberties Union commented on the events: "Even if the Hungarian law on promulgating the PNR agreement includes provisions on asking for the passengers' consent for handling their personal data, it won't be very useful. How can anybody regard the consent as freely given when the passengers are not allowed to board or disembark the airplane without providing?" ibid.

[33] Ibid.

10. Traffic data & Electronic trails

Any type of data base that generates electronic trails (for e.g., the telecommunication networks, cellular telephone systems, consumer oriented funds transaction systems and automatic traffic control systems) can be used for surveillance purposes – the classical example is the use by the German police of the billing records of the Hamburg electrical board to locate the terrorist Rudolph Clemens Wagner. The police (especially in Germany) had been using traffic data to locate terrorists since the seventies. The lessons of the Clemens Wagner case from the Baader-Meinhof era were well-learnt.

Post-9/11 the police and security forces became more acutely aware of terrorist and crime uses of the Internet. To them the Internet is simply another communications system "to tap" and especially to provide "traffic data". One may consider however the distinction between the uses of data base surveillance for locating an individual (as in the case of Rudolph Clemens Wagner), and the use of surveillance for analysis with the objective of identifying a suspect population.[34]

"When the police are looking for a terrorist, any source of information may be relevant. There are traditional procedures to be followed for obtaining this information similar to those governing search and seizure procedures. The crime in known, the interest in solving the crime may be balanced against, for instance, the interest in privacy. This may be termed *individual data base surveillance*. More difficult is the *collective data base surveillance* situation where no suspect has been identified prior to the data base surveillance..."[35]

A regulation of the collective data base surveillance is not mainly an issue from the perspective of the individual data subject, but is part of a broader issue – the level of surveillance that should be accepted in a society, what procedures should safeguard against misuse of such methods, etc.[36] It is submitted that measures obliging telecommunications and Internet Service providers to store data on all telecommunications and Internet traffic for extended periods are disproportionate and therefore unacceptable. The European Data Protection Commissioners Conference meeting on 6/7 April 2000 in Stockholm stated that such retention of traffic data by Internet Service Providers would be an improper invasion of the fundamental rights guaranteed to individuals by the European Convention on Human Rights.[37]

[34] Prof. Dr. Juris Jon Bing, Privacy and Surveillance Systems – available at http://www.jus.uio.no/iri/forskning/lib/papers/privacy/privacy.html

[35] Quoted from the memoirs of Jan Freese, who was head of the Swedish Data Protection Inspection at that time, cf Den makfulkomliga oförmogan, Wahlström och Widstrand, Stockholm 1987:97.

[36] Prof. Dr. Juris Jon Bing, Privacy and Surveillance Systems.

[37] Cf. also Recommendation 3/99 of the Article 29 Working Party on the preservation of traffic data by Internet Service Providers for law enforcement purposes.

11. Data Retention – ignoring the principle of "purpose specification"

Discussions on regulating the retention of traffic data for law enforcement purposes go as far back as the G8 meeting in Moscow in 1999. By the year 2000, retention of traffic data was allowed for billing and interconnection payments. 9/11 speeded up the discussions and gave a 'justification' for retention of traffic data for longer periods.

The resistance of the Article 29 Working Party, the EDPS and civil society remained unaltered. Upon several occasions since 1997, the Article 29 Working Party and the Conference of European Data Protection Authorities have questioned the necessity of general data retention measures.

In several of its Opinions and Recommendations, the Article 29 Working Party has repeated, almost as a mantra, that retention of traffic data for purposes of law enforcement should be allowed only under strict conditions and that the retained data should only be kept for a limited period and only where necessary, appropriate and proportionate in a democratic society. In its **Opinion on the Draft Data Retention Directive**[38] the Article 29 Working Party questioned whether the justification for any compulsory and general data retention coming from the competent authorities in Member States had been clearly demonstrated and backed up with evidence and also whether the proposed data retention periods in the draft Directive were convincing. The Working Party also stated that in any case, the conditions under which the competent authorities could access and use such data in order to combat the threat of terrorism should be clearly spelled out. Yet, in spite of the Opinion of the Article 29 Group and protests form many other quarters, the European Union still brought into effect Directive 2006/24/EC – The Data Retention Directive.

This Directive forces, in an unprecedented manner, providers of publicly available communication services to store trillions of data relating to the communications of any and all citizens for investigational purposes. So, although it is submitted that the right to respect for private life implies that not everybody can indiscriminately become the subject of criminal intelligence, European law now makes it legitimate (indeed mandatory) to create the tool necessary to make everybody indiscriminately the subject of criminal intelligence-gathering activities.

In the aforementioned Opinion the Article 29 Working Party set out specific safeguards to be envisaged with particular regard to the requirements applying to recipients and further processing, the need for authorizations and controls, the

[38] Opinion WP113 of 21 October 2005

measures applying to service providers also in terms of security and logical separation of the data, the determination of the data categories involved and their updating, and the need to rule out contents data. One could say that the Article 29 Working Party's 'list of desirables' constitutes a return to basic data protection principles and in this sense preserve the spirit of R(87)15. *A contrariu sensu,* the extent to which the specific safeguards were addressed or ignored in Directive 2006/24, may be considered to be a measure as to how much R(87)15 is being "killed softly":

1. *Purpose specification* – Directive 2006/24 does not clearly define and delineate the specific purposes for which data should be retained. Rather, it mandates that the retained data must be made accessible to authorities investigating on non-specified "serious crimes". Thus, the sacred principle of purpose specification, so hard-fought to achieve in R(87)15, has been ignored.

2. *Access limitation* – Directive 2006/24 provides that the retained data is to be provided only to the competent national authorities, but it does not further provide that the competent national authorities should be specifically designated law enforcement authorities or that a list of such designated authorities should be made public. Neither does it clarify that other stakeholders, like the provider himself, do not have access to the data or that the data can only be provided if this is needed in relation to a specific criminal offence.

3. *Data minimisation* – Directive 2006/24 defines data categories in Art 5.

4. *No data mining* – The limitation in Art 4 of 2006/24 to "specific cases" seems to prohibit data mining activities. However (unlike much of the thrust in R(87)15) the Directive does not specify that the retained data can only be provided if this is needed in relation to a specific criminal offence.

5. *Further processing* – contrary ot the opinion of the Art 29 Working Party or the thrust of R(87)15, Directive 2006/24 contains no provision ruling out or limiting stringently further processing for other related proceedings.

6. *Access Logs* – Contrary to the opinion of Art.29 Working Party, the Directive 2006/24 does not create safeguards by providing that any retrieval of the data should be recorded and the records made available to the supervisory authority.

7. *Judicial / independent scrutiny of authorized access* – Once again, an important safeguard recommended by the Art. 29 Working Party is not mandated by the Data Retention Directive.

8. *Retention Purposes of Providers* – Yet again in breach of the advice of the Art.29 group, Directive 2006/24 does not provide safeguards by specifying that data should be retained by the service providers solely for public order purposes, and not for other purposes, especially their own.

9. *System Separation* – There is no specific provision in Directive 2006/24 mandating, in particular, that the systems for storage of data for public order purposes should be logically separated from the systems used for business purposes and protected by more stringent security measures.

10. *Security Measures* – Although Article 7 of Directive 2006/24 lays down general requirements on minimum standards concerning the technical and organisational security measures to be taken by providers, these are not sufficient and in particular the relationship between the adequacy of safety-measures and the costs is not addressed in the text of the provision.

Thus, not only did the Data Retention Directive completely ignore the basic principle of purpose specification, on at least eight other counts, the Directive has been found to fail in providing important safeguards in what constitutes a huge new international collection of databases of transaction data.[39]

Directive 2006/24 has been the subject of harsh criticism, *inter alia* for the disproportionate nature of its measures, for the fact that the notion of purpose is not respected, not enough safeguards established and the cost-efficiency of data retention is nowhere demonstrated.

In its Opinion 3/2006 of 15 March 2006, the Article 29 Working Party remained critical of the Directive, particularly in view of the fact that it lacks some adequate and specific safeguards and leaves room for diverging interpretation and implementation by the Member States. The Working Party considered it crucial that the provisions of the Directive are interpreted and implemented in a harmonised way and that the Directive is accompanied in each Member State by measures curtailing the impact on privacy.

[39] Most of these deficiencies had also been anticipated by Hustinx. On 26th September 2005 Peter Hustinx, European Data Protection Supervisor (hereinafter referred to as the EDPS), issued his Opinion on the Proposal for a Directive on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC39 (hereinafter referred to as the Opinion on the Proposed Data Retention Directive).

12. The Verdict: Is R (87) 15 dead or is it dormant?

It is submitted that the Data Retention Directive achieves the death (or at least a comatose state) of "purpose"...but only for traffic data. The respect for the principle of purpose for gathering data, in this case "traffic data", now takes second place to the notional usefulness of such data in the fight against terrorism and crime. The danger inherent in having whole masses of data preserved, for years and subject to the monitoring by the police and security forces for "their" purposes is being ignored. The Data retention directive lowers the standards by giving legitimacy to the opponents of "purpose" and creates new dangers in the form of large databases of traffic data which previously did not exist.

This being said, strictly speaking R(87)15 is neither dead nor dormant. It is still applicable in every area of personal data except communications traffic data. It still retains all its original strengths as well as its intrinsic weaknesses. As a mere Recommendation, it has no binding power on the member states of the Council of Europe. Quite simply, Hustinx is right in identifying a lacuna and the equivalent of R(87)15 needs to be written into EU law. For there can be no doubt that R(87)15 had achieved a degree of international consensus within Europe. Whether a renewed commitment to this consensus will take the shape of a new Convention of the Council of Europe or an Additional Protocol to Convention 108 incorporating R(87)15 or a new EU Directive adopting as much of R(87)15 as a fierce internal debate will allow (or at least two of the previous options) remains to be seen.

Whichever way it goes, it can also be viewed as being part of a cycle or even a cycle of cycles. The data protection debate is not dead either. While the wars in Iraq and Afghanistan have done much to keep international public attention focused on the so-called "war on terror" and this may have possibly contributed to the data retention directive being introduced in spite of it's clear incompatibility with key established principles like "purpose", there is no clear evidence that a "terror-weary" European public will not once again give prominence to the right to privacy. For the cycles in European history have shown that while terrorism cannot be defeated, nor can it be victorious for it can be contained.[40] In the carnage wrought by roadside bombs and suicide bombers in Iraq and Afghanistan, more Europeans will recall that many of these tactics had been perfected in the "culvert" bombs of the IRA which drove British troops off the road in areas like South Armagh and had forced a total reliance on helicopter transport until troop withdrawal in 2006.

Historical cycles have shown that while terrorist activities will not disappear, there will often be long patches when they fade into the background and new, fresher issues will take their place. Already, the Montreal 2007 Conference of

[40] A lesson learnt from the IRA struggle

Data Protection & Information Commissioners is set to focus further on the Surveillance Society and the ID card is possibly one of the issues that may take some of the limelight during the next national election in the UK. Fundamental Human Rights were one of the planks of Labour policy in the pre-1997 electoral campaign and privacy may yet return to a cycle of being in fashion. At this moment in time, much is being forgiven and/or forgotten in the name of security but when the public realizes or is persuaded that the very same security-measures may be posing a threat to cherished liberties, then we may be in for another cycle of change.

The future of surveillance technologies is probably rosy but not as clear-cut so as some may think. While the mayor of Chicago is promising a CCTV camera on every street corner by 2016, openly boasting that Chicago would rival London, on the other hand Detroit, Miami and Iowa have all abandoned their camera surveillance systems because they did not cut down on crime.[41] The future of R(87)15 will depend on another "battle for hearts and minds" – that of persuading voters that unregulated technological surveillance and unfettered police use of personal data cannot be tolerated. As in the case of R(87)15 in 1984-1986, this debate can be won if it is undertaken by the right people using the right means at the right time. In the same way that 9/11 lent fuel to the Data Retention Directive, it cannot be excluded that some other incidents will not lend themselves to advocates of a new EU Directive implementing R(87)15. There exists a precedent in the way that EU 46/95 practically legislated Convention 108 into being across Europe, in the teeth of some strong opposition, particularly from the UK. A repeat performance with R(87)15 would help temper but possibly never completely exclude the nightmare scenario painted by Richard Thomas i.e that of our sleepwalking into a surveillance society..

It is interesting to speculate on the effect that a resurrected European constitution could have on the fate of R(87)15. The recent "yes" vote in Luxembourg and German premier Merkel's undertaking to resurrect the constitution may lead to developments favourable to R(87)15 if the constitution were to retain its current positive bias towards data protection ruled. In such an eventuality, there is a case to be made for the Data Retention Directive to be un-constitutional, provided always that by the time the Constitution comes into being, EU 2006/24 would not have been scrapped on account of its not being cost-effective.

[41] http://www.epic.org/privacy/surveillance/

10/31/2010

Appendix Three

Data Protection Vision 2020

options for improving European policy and legislation during 2010-2020

Joseph A. Cannataci

2010 Fourth International Conference on Digital Society

Squaring the Circle of Smart Surveillance and Privacy

Joseph A. Cannataci
Centre for Law, Information and Converging Technologies
University of Central Lancashire
Preston PR1 2HE, United Kingdom
e-mail: JACannataci@uclan.ac.uk

Abstract*—This paper finds that recent growth in investment in CCTV surveillance technology is in inverse proportion to its relatively very low rate of effectiveness in combating crime and terrorism. It maintains that the much-publicised failures of some smart surveillance technologies such as automated face recognition in the period 1997-2003 has led to investment in even "smarter" technologies of a type here categorised as MIMSI (Massively Integrated Multiple Sensor Installations) which link up optical-based technologies such as CCTV to other sensory detectors involving scent, sound and motion. After having outlined the risks inherent in new surveillance technologies and their applications, the paper moves on to examine the paucity of legal safeguards currently available for the protection of the privacy of citizens. This analysis serves as the context for the final part of the paper which focuses on the European Union's Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters. The latter purports to provide a safer way in which personal data may be exchanged between the police and security forces of European Union states. This paper finds that the CFD 2008/977/JHA sets out an extremely important principle relevant to smart surveillance but then does nothing to actually provide concrete safeguards for citizen privacy.

Keywords-privacy, smart surveillance, CCTV, MIMSI, data protection

I. INTRODUCTION –CURRENT SITUATION IN CCTV

In a society where it is so fashionable to be "evidence-based", it is difficult to bridge the gulf between the evidence on the effectiveness of CCTV surveillance and the apparently increased resolve of politicians and security operators to invest in more and more expensive CCTV-led surveillance systems. On October 4 2009, the Mayor of New York and his Police Chief led a press conference [1] to announce that they were extending the Lower Manhattan Security Initiative (LMSI) to the Middle Manhattan Area. The cost of the extension was declared to be funded by 24 million dollars from federal Homeland Security grants, building upon a system which for years had been declared to be modelled on London's "ring of steel" [2].

If London were truly the model for New York, it is not clear whether Mayor Bloomberg and his advisors had taken note or ignored of what was actually being said by senior police officers in London who in 2008 had declared "the system was an "utter fiasco" - with only 3% of London's street robberies being solved using security cameras" [3]. Indeed, barely a month before Mayor Bloomberg and Police Chief Kelly held their October 4 2009 Press conference on Middle Manhattan, in London Detective Chief Inspector (DCI) Neville, the head of the Metropolitan Police's Visual Images, Identifications and Detections Office (Viido), admitted "just 1,000 crimes were solved in 2008 using CCTV images, as officers fail to make the most of potentially vital evidence" [4]. With more than a million CCTV cameras in a London where the Government has spent £500 million on the crime-fighting equipment this works out at less than one crime solved per 1,000 cameras per year.

DCI Neville's public statements of August 2009 and May 2008 cited above were important confirmation of existing impressions but hardly news for surveillance experts. Instead they corroborate a solid body of evidence coming from different quarters that CCTV surveillance does little or nothing to deter crime and was only of disproportionately limited use in solving crime *post factum*. In February 2009, the American Civil Liberties Union (ACLU) was (largely accurately) reporting that "The two main meta-analyses conducted for the British Home Office show that video surveillance has no impact on crime whatsoever" [5]. This despite a slightly more positive meta-analysis (also Home Office-funded) published less than two months previous which held that "Results of this review indicate that CCTV has a modest but significant desirable effect on crime, is most effective in reducing crime in car parks, is most effective when targeted at vehicle crimes (largely a function of the successful car park schemes), and is more effective in reducing crime in the United Kingdom than in other countries" [6].

Anybody reading this assessment would understand any investment of CCTV in car parks but close scrutiny of the latest developments in New York suggests that surveillance is no longer a matter of limited CCTV operating in isolation or that new investment is confined to car parks. Instead one finds New York's 250 crime-fighting cameras have, in the space of two years, been increased more than tenfold to 3,000 and that the public sector is now increasingly able to access private sector CCTV installations. Perhaps even more important than the scale of the increase in the number of the CCTV cameras is however the fact that they are no longer designed to operate in isolation but are part of a massively integrated system. The LMSI "consists primarily of closed

978-0-7695-3953-9/10 $26.00 © 2010 IEEE
DOI 10.1109/ICDS.2010.55

circuit television (CCTV) cameras, license plate readers, and chemical, biological, and radiological sensors" [7].

New York is not the only major US city to take such a comprehensive approach to surveillance. Chicago's Operation Virtual Shield project is an incredibly elaborate multi-tiered hardware and software approach which after laying down its own fibre-optic networks around the city, between Nov 2008 and Feb 2009 has linked up the CCTV to the 911 emergency network. When the ACLU raised privacy concerns about the new Chicago system, it was reported that "Some experts, including Albert Alschuler, a law professor at Northwestern University, say the surveillance cameras and updated 911 system do not violate privacy rights because the cameras are installed in public locations. Mr. Alschuler said: "My more serious concern would be if they start using new audio technologies, which can be calibrated to alert police to loud noises, like a scream or a car crash. What worries me is if police can use technology to listen to anyone who happens to be talking in a public location, which would raise serious privacy concerns" [8].

Alschuler may have been very timely in airing such concerns since just two weeks previous, a system in Scotland had just gone on trial precisely to listen to sounds of trouble on a Glasgow street. A Dutch company called Sound Intelligence carried out a two week long trial of their system, Sigard, in a busy city centre street. The system does not record conversations and listens not to what is being said but how it is said. It is able to discriminate between the sound of aggression and other everyday loud noises like passing trucks [9].

New York and Chicago's recent heavy investment in increased surveillance technology flies in the face of a sustained and concerted campaign by the ACLU to stop widespread use of CCTV. Indeed, after the Tampa Florida Police suspended use of automated face recognition CCTV in 2002 [10] the ACLU continued to publicise a list of failures of CCTV around the United States and the rest of the world. Under no illusions that it was winning the war for hearts and minds, in January 2009 it launched a specific web-site YouAreBeingWatched.us and by May 2009 was suing the NYPD for details of LMSI [11]. While across the border in Canada, Vancouver City hall voted to introduce CCTV for security during the 2010 Olympics [12], in June 2009, the ACLU was able to celebrate a small victory just north from New York when the local Community in Brookline in the Greater Boston area voted to reject the use of additional CCTV cameras even though they would be paid through Homeland Security funding [13].

Even if the Brookline example shows that when communities are given a choice some now appear to be willing to reject increased use of CCTV, where no citizen choice is available the situation appears to have grown darkly different. While it has been generally believed that the UK is the world's most spied upon society with more than 4.2 million cameras for 60 million inhabitants, it does not seem destined to hold that title for long. For the shape of things to come we may wish to look east and specifically to the place where so many of the new CCTV cameras are built: China. In September 2009 it was reported that in Guangdong province alone the state has "already installed more than 900,000 video cameras in Guangzhou, Shenzhen, Zhongshan, Dongguan, Chaozhou, Zhuhai and other major cities in the Pearl River Delta, which borders Hong Kong and Macao special administrative regions" [14] and "over the next three years, Chinese security executives predict they will install as many as 2 million CCTVs in Shenzhen, which would make it the most watched city in the world" [15]. While nowhere near Chinese developments, the number of CCTV cameras in Paris is also expected to quadruple within one year by end 2009 [16] as part of a drive to "triple" the existing CCTV surveillance capacities across the country, "with a view to curb the risks of terrorism and acts of violence" [17].

II. ENTER MIMSI

From a technological viewpoint, what is most interesting in the development of CCTV surveillance over the past ten years has been the move away from those very same defects that made CCTV look like a privacy-intrusive technology which was not cost-effective when it came to deterring and solving Crime. Firstly, the blurred, grainy out-of-focus images taken from the wrong angle and which have so often upset policemen like DCI Neville [18] are being replaced or complemented by those from high definition (HD) Pan Tilt and Zoom (PTZ) models located at all angles working in conjunction with better-positioned HD fixed models, often with capacity for on-board video analytics. Secondly, where a dedicated or secure communications network is not immediately available, suppliers are now using cameras which can transmit and be controlled using Internet Protocol (IP). Thirdly, if a city or corporation had already invested in installing and maintaining a considerable number of analog cameras, the suppliers can insert a layer of software that can deal usefully with images from those cameras. Fourthly, some cities or other major users (but not all) have opted for new and varied forms of video analytics which do not necessarily rely on previously less reliable technology like face recognition but which identifies potential risks in other ways of analyzing the video signal. Fifth and perhaps most importantly, system designers are not relying on video alone but are increasingly bringing in audio and indeed other signals from every possible type of sensor imaginable and analyzing them.

Within new project design work [19] initiated by our research centre, we have categorised this new phenomenon as the *Massively Integrated Multiple Sensor Installations* (MIMSI) approach to surveillance. To put it differently, supposedly "smart" technology (such as automated facial recognition) was perceived to be failing and needed to become even "smarter". The dual approach of different novel forms of video analytics and less reliance on optics through large scale integration means that one of the key technology areas that privacy lawyers now need to deal with is MIMSI.

When surveying recent surveillance developments in Beijing, Chicago, New York and Shenzhen the common denominator is MIMSI and in at least three of these cities,

the company providing the smart technology is the world's largest IT company IBM. While IBM is a great propagator of everything "smart" [20] and is quick to point out the advantages of a MIMSI approach to less controversial applications such as water and electricity management [21] it has also overtly integrated its SMART S3 technology in both Beijing and Chicago's public CCTV systems and is reportedly also set to do so in New York [22] with inroads already made into Italy's UNICredit bank and other sites internationally [23]. However, the effectiveness of integrating data from several sensors into one system has been questioned by some commentators [24] They point out that while using multiple sensors/detectors can be effective, it is difficult to predict the number and kinds of detectors (e.g. are radiation detectors enough when terrorists can resort to dynamite?) needed in any particular situation. The logical answer may be to use all necessary sensors/detectors that are successful in detecting and displacing (if not deterring) crime when used in combination with CCTV [25] and if they are less privacy-intrusive than other sensors but more effective in countering real threats then they may indeed be a preferable investment in high risk areas.

For other commentators the issue simply lies with business opportunities opened up by MIMSI. If sometimes privacy does not seem to be at the top of some people's concerns, the answer may possibly be in the figures. In terms of business alone the situation may be summarized as follows: in 2009 the Chinese internal-security market is worth an estimated $33 billion — "around the same amount the US Congress has allocated for reconstructing Iraq" while "The global homeland-security business is now worth an estimated $200 billion — more than Hollywood and the music industry combined" [26]. The momentum achieved by such a global business inevitably means that every entrepreneur who may sell his/her new sensor to a MIMSI-type surveillance system will try to do so, and often succeed, feeding on fears provoked by every new emergency or terrorist attack. The business opportunities offered by MIMSI are not lost on entrepreneurs. In Shenzhen, "the cameras that Zhang manufactures are only part of the massive experiment in population control that is under way here" [27]. The big picture is integration: the linking of cameras with other forms of surveillance such as the Internet, phones, facial-recognition software and GPS monitoring [27].

III. MIMSI IN CHINA

Before proceeding to examine some of the legal aspects of MIMSI it is instructive to note the technological capabilities of the level of integration. Commentators argue that "Chinese citizens will be watched around the clock through networked CCTV cameras and remote monitoring of computers. They will be listened to on their phone calls, monitored by digital voice-recognition technologies. Their Internet access will be aggressively limited through the country's notorious system of online controls known as the "Great Firewall." Their movements will be tracked through national ID cards with scannable computer chips and photos that are instantly uploaded to police databases and linked to their holder's personal data. This is the most important element of all: linking all these tools together in a massive, searchable database of names, photos, residency information, work history and biometric data. When Golden Shield is finished, there will be a photo in those databases for every person in China: 1.3 billion faces" [28].

It is also important to note that while the NYPD declares in its (non-binding) guidelines that it will not be using face recognition technology [29], the Chinese have no such qualms and indeed in 2008 were busy conducting tests aimed at integrating face recognition into their nationwide surveillance system [30]. The UK seems to have of late overcome some of its earlier hesitancy over face recognition technologies (FRT) since "only recently have they become reliable enough to be deployed on a large scale" [31].

It is equally instructive to note that it has been claimed that integrated technologies have already led some Chinese dissidents to flee their homeland. "Internet cafes used to be a place in China where people could use the Internet with some degree of anonymity and that's really been eroded… Every time he went to an Internet cafe, he needed a special ID. The Internet cafe takes your national ID and then issues a card for you that's linked to your national ID, so every time you're logged onto the Internet, you're scanned and if you're on a list an alarm will go off somewhere because the alarm is linked in to local police. It's clear that it's not just the cameras feeding directly into local police; it's the computer themselves." [32]. Somebody could suffer from surveillance of Internet use, that is, if he were ever allowed to use the Internet in the first place. In an integrated system with a centralized database feeding to local watchdogs (local or provincial police) controls can be applied to anything from booking into a hotel or even trying to use the Internet [33].

The level of integration is now so high and the level of crackdown on free use of the Internet in China is apparently so acute that on October 8 2009, 15 Chinese intellectuals, including writers, scholars and lawyers, jointly issued the "an online Internet Human Rights Declaration" reinstating the citizen's rights to access and disseminate information" [34]. The main problem of course is that it has been claimed that the same type of integrated control may mean sanctions for any Chinese lawyer who tries to tackle these issues [35].

IV. MIMSI GOES WEST

The space afforded by this short paper does not permit one to delve further into the privacy and other legal aspects of MIMSI in China where certain elements of public policy may be different to that within the EU and North America. This paper now attempts to identify which legal safeguards have been put in place to prevent MIMSI in western democracies from constituting the same threat to fundamental rights and democratic values as would prima facie appear to be inherent in, say, the Chinese approach to and uses of integrated surveillance systems. Back in "the West", as has been seen above, MIMSI is making significant inroads in places like New York and Chicago but despite vociferous complaints and the occasional law-suit by civil

liberties groups, when it comes to surveying the legal framework within which MIMSI operate, a common defense advanced is that 'whatever goes on in a public space is not subject to any constitutional rights on privacy'. In spite of this, it is clear that some police authorities like NYPD are moderately sensitive to the privacy concerns of citizens. The NYPD in February 2009 published a draft set of guidelines inviting input in the course of what was outwardly a public consultation exercise. By October 2009 the Guidelines appear to have been adopted and the NYPD claim that they are "first-of-a-kind". Certainly, at first glance, they contain some interesting points. Firstly it is interesting to note that the NYPD nomenclature for MIMSI is a Domain Awareness System (DAS) for which they find the widest possible definition: "technology deployed in public spaces as part of the counterterrorism program of the NYPD's Counterterrorism Bureau, including: NYPD-owned and Stakeholder-owned closed circuit television cameras (CCTVs) providing feeds into the Lower Manhattan Security Coordination Center; License Plate Readers (LPRs); and other domain awareness devices, as appropriate." [36]

Having included practically every device under the sun, the Guidelines go on to make two important qualifications: "The Domain Awareness System will be used only to monitor public areas and public activities where no legally protected reasonable expectation of privacy exists. Facial recognition technology is not utilized by the Domain Awareness System" [37]. Having made these two explicit statements clearly aimed at placating members of the public concerned with privacy or pre-empting any reminders of past police failures with FRT, it is also interesting that at first glance, the Guidelines seemingly conform to the notion of "purpose" fundamental to European data protection law (where data gathered for one purpose may only be used for the same or a compatible purpose). In Section IIB they explicitly contain a Statement of Purpose which assures the reader that "The Domain Awareness System is a counterterrorism tool designed to: Facilitate the observation of pre-operational activity by terrorist organizations or their agents; aid in the detection of preparations to conduct terrorist attacks; Deter terrorist attacks; Provide a degree of common domain awareness for all Stakeholders; Reduce incident response times; Create a common technological infrastructure to support the integration of new security technology" [38]. Note that "integration", key to the concept of MIMSI is a stated, explicit and relatively unrestricted aim of DAS and that a closer reading of later sections actually permits the NYPD to use the data gathered for any legitimate police purpose (with minimum inconvenience to them and minimalistic safeguards).There are also effectively no real limits to the extent to which the DAS may be integrated with other systems "In certain cases, technologies governed by the Guidelines may utilize or be integrated with systems and technologies deployed by other bureaus and divisions of the NYPD" [39]. In which case all we are told that they will be regulated by another memorandum (not these Guidelines). There is provision in the Guidelines for data sharing with any kind of third party (not even necessarily a police or security force)-all an overseas police force requires is a Memorandum of Understanding and the data sharing is authorized in terms of the Guidelines [40]. The section providing sanction is as weak and vague as they come simply stating that "appropriate disciplinary action will be taken" which is not much deterrence to abuse of the system by any officer.

So with a blank cheque to integrate at will to use the system for any kind of legitimate police work, what kind of legal constraints are actually placed upon the NYPD's use of DAS? A saving grace is a clear policy statement on the duration for which data shall be stored and kept [41] but it should be clear that the Guidelines have no force of law and are little better than a non-binding Statement of Intent. This is made amply clear in the concluding part of the Guidelines which state "Nothing in these Guidelines is intended to create any private rights, privileges, benefits or causes of action in law or equity" [42]. So much therefore for any hopes that an aggrieved citizen may have had of exacting redress from the NYPD in pursuance of a "first of a kind" document.

This has been recognized by the ACLU lead counsel on the LMSI case [43] as well as some of the local lawmakers. One councilman, whose lower Manhattan district includes the designated area, was quoted as saying that he views the NYPD's guidelines as a first step toward ensuring that video surveillance is done properly and it is important that this not allowed to evolve into a general surveillance system, but rather be used to identify and prevent real threats [44]. The same councilman plans to introduce legislation that would codify regulations and restrictions for video surveillance in the five boroughs. [44]. When doing so, lawmakers in the US have a number of choices to make. They could do worse than examine the report and model legislation drafted by the not-for-profit Constitution Project and published in 2007 in Guidelines for Public Video Surveillance [45] though to date it would appear that less than a handful of US municipal lawmakers have actually enacted statutes regulating video surveillance [46]. They would also do well (and possibly better) to look across the Atlantic and find out what the Europeans have been up to.

The Council of Europe had fully 22 years ago adopted a seminal Recommendation on the use of personal data for police purposes [47]. Although technically not binding for the 47 member states of the Council of Europe, R(87)15 attained significant importance when it was in 1997 adopted as the data protection standard for the EU's Schengen Agreement. As the EU moves closer to an ability to legislate further on Justice and Home Affairs issues with the recent steps to implementing the Lisbon Treaty, it would not be unreasonable to expect that much if not all of R(87)15 would be transformed into a binding part of EU law. Of particular note in this instance is that part of R(87)15 which would deal with smart surveillance, especially since a characteristic of the latter is the automation of part or all of the decision-making process in surveillance. As has been noted in many works on police surveillance work, two of the key problems addressed by automation of video analytics include i. the sheer volume of data generated by a massive amount of cameras and sensors and ii. the inability of VDU operators to retain concentration on the job of watching multiple images

on multiple screens. This is where the smart software becomes mission-critical to law-enforcement: it needs to be able to sort the wheat from the chaff and direct attention of a human operator when a pre-determined risk situation is identified. To this extent the smart system is already taking a decision in an automated manner. The extent to which it can continue to set in motion a whole range of responses in an automated manner depends very much on the way the system is set up.

The Council of Europe (and its data protection heir, the European Union (EU)) has long had a strict line on the non-acceptability of having automated decisions taken with significant impact on data subjects and R(87)15 is no exception. Section 2.3 of the Recommendation explicitly lays down that "The collection of data by technical surveillance or other automated means should be provided for in specific provisions". Unlike the general licence on integration afforded in the NYPD Guidelines, Section 5 of R(87)15 is far stricter "The interconnection of files with files held for different purposes is subject to either of the following conditions: a. the grant of an authorisation by the supervisory body for the purposes of an inquiry into a particular offence, or b. in compliance with a clear legal provision. Direct access/on-line access to a file should only be allowed if it is in accordance with domestic legislation which should take account of Principles 3 to 6 of this recommendation" [48]. A glaring difference between the European data protection regime and the NYPD guidelines is the right of access, rectification and erasure of personal data granted to data subjects in Principle 6 of R(87)15 but which is nowhere contemplated in the New York guidelines.

Easily the most interesting recent legal development pertinent to the level of automation inherent to smart surveillance systems such as MIMSI is the EU's Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters" and especially where on reads in Article 7 captioned "Automated individual decisions"

"A decision which produces an adverse legal effect for the data subject or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to the data subject shall be permitted only if authorised by a law which also lays down measures to safeguard the data subject's legitimate interests" [49].

While currently applicable only to data exchanged between states (though the pressure is on that this rule like others will later become applicable to all forms of police data within the EU), this regulation would *prima facie* mean that any smart surveillance system would only be able to be operated if there exists a specific law authorizing such use which in turn must lay down specific safeguards "to safeguard the data subject's legitimate interests". At this moment in time, it is not only New York or Chicago which lacks such a law but indeed most if not all of the European Union's 27 member states. Essentially CFD 2008/977/JHA lays down what is on the face of it quite a strict rule but since it does not provide any concrete examples of the types of safeguards that its drafters had in mind it still leaves EU member states some way to travel before they can be in compliance. So the public policy quandary about smart surveillance would, in the EU, appear to have been resolved by international agreement which requires every member state to have in place a specific law which explicitly authorizes automated systems such as smart surveillance and which just as explicitly spells out the legal safeguards for data subjects affected by such systems. Member states have as yet no model law or detailed guidelines on how to achieve this objective (certainly CFD 2008/977/JHA does not provide this) but perhaps help is at hand: by 26th November 2009 the European Commission is expecting to receive offers for research projects aimed at possibly filling such a void in an effort to strike the right balance between smart surveillance on the one hand and privacy and data protection on the other. As to whether such research would actually, by 2014, produce a model law in full compliance with CFD 2008/977/JHA remains a moot point. Even it if were to do so, the extent to which it would become a model to be adopted across the Atlantic, never mind in China, remains doubtful, given US reluctance to follow any kind of European lead on privacy and data protection law.

REFERENCES

[1] Comprehensive Counterterrorism Program to Fortify New York City Financial District Will Include Midtown Manhattan, Press Release 04 October 09 at <http://www.nyc.gov/html/nypd/html/pr/pr_2009_028.shtml> 30.11.2009

[2] Alison Gendar, "Lower Manhattan Security Initiative up and running, safe from budget cuts" in NY Daily News of 24 Nov 2008.

[3] "CCTV boom failing to cut crime" Story from BBC News 06 May 2008 <http://news.bbc.co.uk/go/pr/fr/-/2/hi/uk_news/7384843.stm> 30.11.2009

[4] Mark Hughes, "CCTV in the Spotlight: one crime solved for every 1,000 Cameras" in The Independent, 25 August 2009.

[5] Noam Biale, "What Criminologists and Others Studying Cameras Have Found", American Civil Liberties Union accessed 09 October 2009 at <http://www.youarebeingwatched.us/about/182/> 30.11.2009

[6] Brandon C. Welsh, David P. Farrington "Effects of Closed Circuit Television Surveillance on Crime" The Campbell Collaboratrion 2 December 2008, p.2 DOI 10.4073/csr.2008.17

[7] Comprehensive Counterterrorism Program op. cit. [1].

[8] Karen Ann Culotta, "Chicago links street cameras to its 911 network" The New York Times, February 21 2009

[9] Kenneth Macdonald, "CCTV cameras listen for trouble" Story from BBC News 13 February 2009 <http://news.bbc.co.uk/go/pr/fr/-/2/hi/uk_news/scotland/7886656.stm> 30.11.2009

[10] Poor Performance of Tampa's Face-Recognition Technology) ACLU Press release 03 January 2002 <http://www.aclu.org/privacy/spying/14866prs20020103.html> 30.11.2009

[11] New York Civil Liberties Union, "NYCLU Sues NYPD for Information on Massive Surveillance Plan," Press Release, 08 September 2008

[12] Irwin Loy, "City votes for CCTV Surveillance for 2010 Olympics" April 1, 2009 <http://www.no2010.com/node/914> 30.11.2009

[13] "Brookline Rejects Homeland Security Surveillance Cameras" ACLU Press release 03 June 2009 < http://www.aclu.org/privacy/spying/39921prs20090603.html> 30.11.2009

[14] "Guangdong crimes come into focus thanks to video cameras", China Daily on 05 September 2009 <http://www.chinadaily.com.cn/china/2009-09/05/content_8658757.htm> 30.11.2009

[15] Naomi Klein, "China's All-seeing Eye", The Rolling Stone, Posted May 29, 2008 3:24 pm <http://www.rollingstone.com/politics/story/20797485/chinas_allseeing_eye> 30.11.2009

[16] Daily Telegraph 16 October 2008 <www.telegraph.co.uk/.../Paris-to-quadruple-number-of-CCTV-cameras.html> accessed 28 October 2008.

[17] Darren Murph, "France planning to 'triple' CCTV surveillance capacity." Engadget, 28 July 2007 <http://www.engadget.com/2007/07/28/france-planning-to-triple-cctv-surveillance-capacity/> 30.11.2009

[18] "Closed Circuit Television's key role in modern policing," Interview with DCI Mick Neville,Special May Edition at <www.doktorjon.co.uk> 30.11.2009

[19] Joseph A. Cannataci, SMART (Scalable Measures for Automated Recognition Technology) unpublished CLICT project concept document produced for submission to the European Commission in response to Topic SEC-2010.6.5-2 Use of smart surveillance systems, data protection, integrity and sharing information within privacy rules

[20] See various IBM web-pages about smart cities/lifestyle <http://www-05.ibm.com/innovation/uk/think/videogallery.html?ca=sp_videospg_fl&me=w&met=uk_hp_lead> 30.11.2009

[21] "The Tech Lab: Brendon Riley" BBC news 10 April 2009 <http://news.bbc.co.uk/go/pr/fr/-/2/hi/technology/7992480.stm> 30.11.2009

[22] Robert McMillan, "IBM system to scan streets at Beijing Olympics", NYC Created 06 December 2007 <http://www.infoworld.com/print/33801> 30.11.2009

[23] Ibid.

[24] Julia Kantor, "Midtown Manhattan Anti-terror plan to cost $24 million" Epoch Times, Oct 05 2009.

[25] Jeff Roush, "Gun shot detectors: Pushing murder into the next town?" blog posted 13 May 2009 <http://fightingcrimefromabove.com/gun-shot-detectors-pushing-murder-into-the-next-town> 30.11.2009

[26] Naomi Klein, "China's All-seeing Eye", op. cit. [15].

[27] Ibid.

[28] Ibid.

[29] Article C at page 3 of the NYPD Public Security Privacy Guidelines published 02 April 2009 <http://www.nyc.gov/html/nypd/downloads/pdf/crime_prevention/public_security_privacy_guidelines.pdf> 30.11.2009

[30] Naomi Klein, "China's All-seeing Eye", op.cit. [15]

[31] Sean Dodson,"Golden Shield" in ICON 070 April 2009 <http://www.iconeye.com/index.php?option=com_content&view=article&id=3958:gol> 30.11.2009

[32] Q & A with Naomi Klein <http://www.zonaeuropa.com/20080811_1.htm> 30.11.2009

[33] Kuerbanjiang Saimaiti (ıιıι): "Sorry, Your Ethnic Group Can't Use the Internet." China Digital Times 03 October 2009

[34] Global voices Advocacy, "Internet rights declaration" 09 October 2009 <http://chinadigitaltimes.net/2009/10/china-internet-human-rights-declaration/> 30.11.2009

[35] See Professor Donald E Clarke, "Lawyers and the state in China: Recent developments", Testimony Before the Congressional-Executive Commission on China, Washington, D.C.October 7, 2009

[36] NYPD Public Security Privacy Guidelines 02 April 2009 op. cit. [29]

[37] Ibid.

[38] Ibid.

[39] Ibid.

[40] Ibid. at Art C, page 3

[41] Ibid. at Art D page 3-4

[42] Chrsitpher Dunn as cited in "Lower Manahattan: The Eyes have it" 17 March 2009, The Shadowland Journal. <http://christopherdickey.blogspot.com/2009/03/lower-manhattan-eyes-have-it.html> 30.11.2009

[43] Ibid.

[44] Ibid.

[45] NYPD Public Security Privacy Guidelines 02 April 2009 op. cit. [29]

[46] Paul Humphreys, "Video Surveillance on Public Streets: A New Law Enforcement Tool for Local Governments", in NYSBA One on One, Summer 2008, Vol. 29, No.1 mentions Washington D.C and San Franciscio as two of the tiny minority of municipalities which have produced any legislation at all on video surveillance.

[47] Recommendation No. R (87) 15 of the Committee of Ministers to Member States regulating the Use of Personal Data in the Police Sector, Council of Europe, Strasbourg, 1987

[48] Ibid.

[49] European Union Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters Official Journal L 350 , 30/12/2008 P. 0060 - 0071

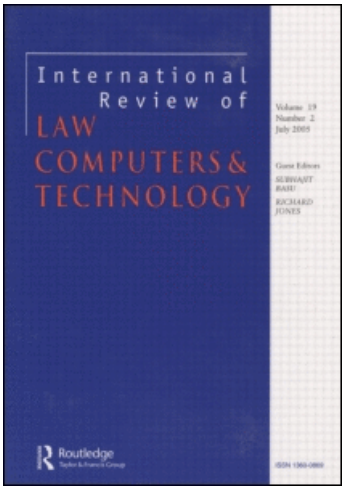
10/31/2010

Appendix Four

Data Protection Vision 2020

options for improving European policy and legislation during 2010-2020

Joseph A. Cannataci



International Review of Law, Computers & Technology
Publication details, including instructions for authors and subscription information:
http://www.informaworld.com/smpp/title~content=t713427052

The end of the purpose-specification principle in data protection?

Joseph A. Cannataci [a]; Jeanne Pia Mifsud Bonnici [b]
[a] Centre for Law, Information and Converging Technologies, University of Central Lancashire, UK [b] University of Groningen, The Netherlands

Online publication date: 02 March 2010

To cite this Article Cannataci, Joseph A. and Bonnici, Jeanne Pia Mifsud(2010) 'The end of the purpose-specification principle in data protection?', International Review of Law, Computers & Technology, 24: 1, 101 — 117
To link to this Article: DOI: 10.1080/13600861003637693
URL: http://dx.doi.org/10.1080/13600861003637693

International Review of Law, Computers & Technology
Vol. 24, No. 1, March 2010, 101–117

The end of the purpose-specification principle in data protection?

Joseph A. Cannataci[a]* and Jeanne Pia Mifsud Bonnici[b]

[a]*Centre for Law, Information and Converging Technologies, University of Central Lancashire, UK;* [b]*University of Groningen, The Netherlands*

The 'purpose specification principle', that is, the principle that a citizen needs to be informed why the personal data is being collected and the specific purposes for which it will be processed and kept, is a central protection for a citizen in data protection law. Data sharing practices using personal data collected for one purpose for another purpose are on the increase with clear prejudice to the purpose specification principle. While initially, at law, data sharing was limited to instances where the purpose for which the personal information is used is not incompatible to the purpose for which the same information was collected, there seems to be a trend to extend instances of data sharing with clear disregard to the purpose-specification principle. This paper documents the proposal and withdrawal of two legislative initiatives (the introduction of data sharing provisions in the Coroners' and Justice Bill 2009 and the Communications Data Bill 2008) to determine whether a clear pattern to end the purpose-specification principle in data protection in the UK is emerging or whether it has in fact seen its end already. The paper argues that while the withdrawal of these legislative initiatives is a positive step even if perhaps instigated by political opportunism, the systematic erosion of the purpose-specification principle will unfortunately continue to increase the possibility of abuse of citizens' rights.

Keywords: purpose specification; data sharing; communications data

Introduction

If 2007 was the year of personal data losses in the UK, then 2008 and 2009 can be recorded as years where most laws having an impact on personal data protection were proposed and withdrawn while massive government programmes using personal data keep on being built (without appropriate legislative basis). This paper documents the proposal and withdrawal of two legislative initiatives (the introduction of data sharing provisions in the Coroners' and Justice Bill 2009 and the Communications Data Bill 2008) to determine whether a clear pattern to end the purpose-specification principle in data protection in the UK is emerging or whether it has in fact seen its end already.

Why focus on the 'purpose-specification principle' and not the rest of the data protection principles? The 'purpose-specification principle'[1] – that is, the principle that establishes that a citizen needs to be informed why his/her personal data is being collected and the specific purposes for which it will be processed and kept – is a central protection in data protection regulation. A citizen's informed consent to the collection and processing of his/her personal data is dependent on the information about the purpose and use of the

*Corresponding author. Email: jacannataci@uclan.ac.uk

ISSN 1360-0869 print/ISSN 1364-6885 online

DOI: 10.1080/13600861003637693
http://www.informaworld.com

personal data. Furthermore, once the purpose is known it is easier for a citizen to trace who is actually responsible for the maintenance of the citizen's information.

As Gellman notes a 'statement of purpose helps to strike a reasonable balance between the interests of record keepers and those of record subjects. It tells the record subject the consequences of disclosing data ... A purpose statement provides the data subject with information about the purpose for data collection, so that he or she can assess the benefits and risks of disclosure and make an informed decision. It also prevents a record keeper from using or disclosing information in ways that are not in accordance with the stated purpose ... The purpose specification principle has a selfbalancing feature.'[2]

Given the importance of the purpose-specification principle in striking and maintaining a balance between the need to collect, use and retain personal information and the data subjects right to respect their private life, it is reasonable to expect that any laws on the use of personal information would give particular attention to this principle. Past experiences, such as in the introduction of the Regulation of Investigatory Powers Act 2000 (RIPA) and the Identity Cards Act 2006, have been criticised as ignoring or watering down the purpose-specification principle.[3] It is important to establish whether the same trend can be traced in the legislative proposals announced, presented to Parliament and then withdrawn during this last year.

Ultimately, the purpose-specification principle is a legal tool that can be used to safeguard deeper fundamental rights of dignity and *lex personalitatis*[4] of individuals in a democratic society. Ignoring or watering down 'purpose' in the collection and use of personal data is an indication that the bigger picture (or human dignity and *lex personalitatis*) is being ignored or worse eroded. The two instances discussed in this paper, unfortunately show that instead of using law (and legal tools, like purpose) to bolster the rights of individuals when technology threatens their dignity, law is being used to water down many of the protections developed between 1984 and 2000.

Data sharing provisions in Coroners and Justice Bill 2009

We start with the most recent proposal and withdrawal: the proposal of the data sharing provisions in the Coroners and Justice Bill given its first reading in the House of Commons on 14 January 2009.

Data sharing within the UK government has been taking place for years but the legality or otherwise of the sharing has not been clarified at all. The Thomas and Walport Data Sharing Review[5] delivered in 2008 lamented the lack of clarity in the legal basis of data sharing and the lack of transparency and accountability of the process. Indeed, their primary recommendations address this lack of transparency and accountability.[6] The report argued that data sharing in itself was not illegal as long as the personal information was used in a compatible purpose to the one for which it was collected. The authors argue that 'As a general rule, it seems right that personal information obtained consensually for a specified purpose should not then be used for an incompatible purpose that goes outside the terms of the original consent. If that were to happen, it would breach the terms of the original consent. For this reason, the second Data Protection Principle, which prohibits reuse of information in any manner that is incompatible with the original purpose, stands as a significant safeguard. It is important to note, however, that "incompatible with" is not the same as "different from". Although some respondents to the review have said that the law should prohibit any reuse of personal information without fresh consent, we believe that returning to people on each occasion when an organisation wishes to reuse personal information for clearly beneficial and not incompatible purposes would impose a disproportionately heavy burden, particularly where the data pool is large.'[7]

They argue further that this data sharing (where the purposes are compatible) is permitted 'so long as robust systems are in place to protect personal information and privacy'.[8]

Given these claims one would expect any legislative proposal in response to this review to increase legal certainty and clearly identify the parameters within which data can be shared between institutions and the purposes for that sharing and the setting up of 'robust systems' to protect personal privacy where personal data is shared. Any legislative provision on data sharing should include, as the Thomas and Walport review points out, two key steps: 'the first is to decide whether it is appropriate to share personal data for a particular purpose. The second is to determine how data should be shared, in particular what and how much data, and by what means.'[9]

In November 2008, the Ministry of Justice issued its Response to the Data Sharing Review Report[10] wherein while agreeing with the recommendations of Thomas and Walport, it promised to 'legislate to create a gateway for data sharing powers, which will be subject to the Parliamentary Affirmative procedure'.[11] The legislative response was presented to Parliament in January 2009 as part of the amendments proposed in the Coroners' and Justice Bill 2009. Hidden among provisions on inquests, murder, infanticide and many other offences, the government proposed to permit the sharing of personal data within governmental institutions. While the Bill did not directly claim that data sharing is permitted, it proposed that when a 'relevant policy objective'[12] so requires 'a designated authority may by order (an "information-sharing order") enable any person to share information which consists of or includes personal data'.[13] At no point in the Bill is a 'relevant policy objective' defined or what it could be. The Bill only said that the authority making the order needs to be satisfied that 'the provision made by the order strikes a fair balance between the public interest and the interests of any person affected by it'.[14] There was no mention in the original Bill on 'purpose-specification principle' or whether the sharing of the personal information was used in a compatible purpose to the one for which it was collected. The drafters seemed to have thought that claiming a 'relevant policy objective' would 'satisfy' any requirement under the second data protection principle (of purpose-specification). The rest of the provisions relate to procedural requirements that need to be followed in the issue of the information-sharing order. These requirements attempt to address the points raised in the Thomas and Walport report on responsibility and accountability.

The introduction of these provisions brought about, as we have already documented elsewhere,[15] much public debate and led to the government withdrawing these provisions on 9 March 2009, within less than two months from the bill being presented to Parliament. What were the main contentions that lead to the withdrawal of the pertinent clauses?

Overriding of purpose-specification principle

A glaring lack of attention to the purpose-specification principle was one of the main contentions. A Research Paper dated 22 January 2009 produced by the House of Commons Library clearly found that: 'New section 50A includes a definition of sharing that explicitly overrides the second data protection principle.'[16] The definition of sharing read:

> (3) For the purposes of this Part a person shares information if the person
> (a) discloses the information by transmission, dissemination or otherwise making it available, or
> (b) consults or uses the information for a purpose other than the purpose for which the information was obtained.[17]

In February 2009, the Information Commissioner commented that 'The wording of Clause 152 is very wide'.[18] He also noted further that 'The UK's data protection legislation implements the European data protection directive (95/46/EC). The UK could well fall foul of its international obligations if it amends or modifies the DPA in such a way that the protection of individuals is undermined.'[19]

Convoluted drafting

The difficulties with the definition of 'information sharing was also highlighted by the Information Commissioner in a Memorandum on the Bill in January 2009:

> The Bill's definition of 'information sharing' will cause considerable difficulty. As it stands, clause 152 says that a person shares information not only if the person discloses the information to another person, but also if the person consults or uses the information for a purpose other than the purpose for which the information was obtained. **This legally convoluted definition will add to the considerable confusion surrounding information sharing. The ICO has to translate the law into simple, sensible guidance for organisations. This definition, which goes against the principle of clarity which lies at the heart of better regulation, will pose a considerable and avoidable obstacle.** 3.4 If the Government believes that there is need to address the use of information for a different purpose, then this should be done through a separate provision, not by stretching the meaning of 'sharing' beyond its normal usage.[20]

Wide and unrestricted information sharing

These wide powers allowed in the bill to government departments to use data collected for one purpose by one department to be used for another purpose by another department generated extensive public interest.[21] Many commentators saw this not only as giving wide and unrestricted powers to government departments but also a first step to possibly allow data sharing also to the private sector.[22] Eight organisations, including the BMA, the Royal College of General Practitioners, the Royal College of Surgeons and the Royal College of Nursing, expressed 'grave concerns' about clause 152. They said that the clause seemed 'to grant the government unprecedented powers to access people's confidential medical records and share them with third parties'.[23]

Indeed the government (itself) acknowledged that the clause as drafted was too wide. Replying to questions put at Committee stage, the Parliamentary Under-Secretary of State for Justice (Bridget Prentice) said '... let me make it absolutely clear, on the record, that I acknowledge that the clause as drafted has the potential to be far wider than it is intended to be',[24] and later in the same debate adds 'one reason why the Bill is drafted so broadly is that it was felt to be difficult to predict every single instance in which an information-sharing order would be necessary. That said, the individual order could be drawn tightly, setting out the classes of information to be shared, who could share them and for what purposes.'[25]

No protection for medical/sensitive information

Another criticism raised to clause 152 (including the amendments proposed at Committee stage) was that the clause did not distinguish between the sharing of personal data and hence no exclusion or added protection for the use of sensitive personal data is given in the clause. It was argued at Committee stage that the sharing of medical information needs to be covered by other provisions. It was argued further that while it 'will often be a big

benefit for medical research in being able to share information, but that the information does not have to be associated with a named individual'.[26]

No safeguards

Another important concern was that the clause provided no checks on sharing of information between government departments. The Thomas and Walport review has specifically recommended that robust systems of protections be introduced in any system allowing information sharing. This recommendation is not only one based on data protection principles, but one which is also dictated/inspired by the massive losses of personal information that had happened during 2007 (and 2008). As one MP put it 'Perhaps it would not matter so much if we could trust this Government and if they have had a good record on handling and storing our data, but can we trust them? I am not going to give the Committee a long list of some of the scandals over the loss of data that have occurred in the past few years, where data have not been properly looked after, but the Government are incompetent.'[27]

Concern on lack of safeguards was also raised by the Joint Committee on Human Rights. In its 8th report, the Committee disagreed with the government's approach to data sharing legislation, which is to include very broad enabling provisions in primary legislation and to leave the data protection safeguards to be set out later in secondary legislation. It said

> **We reiterate our view that, in principle, information sharing powers should be adequately defined in primary legislation, accompanied by appropriate safeguards and subject to the application of the Data Protection Act 1998.**' and '**Ideally, safeguards should be provided in primary legislation. If adequate safeguards were in place in the enabling primary legislation, a narrow fast-track ISO procedure could be a positive development in terms of parliamentary oversight of information sharing proposals, particularly given the limited scrutiny of existing information sharing provisions in primary legislation.**[28]

Amendments to Clause 152

It can be argued that thanks to the public out-cry, by the time Clause 152 of the bill had reached Committee stage on 26 February 2009, two of the amendments to Clause 152 tabled related specifically to purpose.

Amendment 50 added a new sub-section (1A) —

> (1A) No information-sharing order may authorise data to be shared in any way that might result in the date being used for a purpose different from that for which its collection was originally authorised.[29]

and Amendment 52 deleted

> (b) consults or uses the information for a purpose other than the purpose for which the information was obtained.' from the definition of information sharing.[30]

Yet this was not enough to reassure the public or the committee members discussing the clause at Committee stage. Indeed, during Committee proceedings the Parliamentary Under-Secretary of State for Justice (Bridget Prentice) moved to 'to offer Opposition Members the opportunity to sit down outside the Committee, go through the clause again and look at the general principles that we agree on about where data sharing could be a useful tool in improving public services. Let us see whether we can come up with a

more streamlined version that takes into account the fact that Parliament has a role in scrutinising the decisions of Ministers and that in his report the Information Commissioner sees the benefit of removing the current legal barriers. As a result, we will give the people whom we represent better public services.'[31]

Withdrawal of Clause 152

By the first week of March the government moved to shelve the proposals. The Justice Secretary Jack Straw was reported as saying that the 'strength of feeling' against the plans had persuaded him to rethink.[32]

Reflections

There is no doubt that the proposals in the Coroners and Justice Bill on information-sharing ignored the existence of the purpose-specification principle completely. Not only did the provisions proposed not meet any of the recommendations made in the Thomas and Walport report, but they added to the vagueness that already surrounds data sharing between UK government departments.

What is perhaps heartening is that

(1) the public (or more accurately, a number of non-governmental organisations) is clearly aware of the second data protection principle and managed to create enough reaction to the bill to cause the provisions to be withdrawn;
(2) a number of Members of Parliament participated actively in the debate at Committee stage to bring about necessary changes; and
(3) perhaps (or is it too naive to think this?!) the Government has learnt enough from this proposal and withdrawal to give more attention to the data protection principles found in the Schedule of the Data Protection Act.

Communications Data Bill 2008

> Every call you make, every e-mail you send, every website you visit – I'll be watching you.[33]

The Communications Data Bill was announced in May 2008. The declared purpose of the bill was 'to allow communications data capabilities for the prevention and detection of crime and protection of national security to keep up with changing technology through providing for the collection and retention of such data, including data not required for the business purposes of communications service providers; and to ensure strict safeguards continue to strike the proper balance between privacy and protecting the public.'[34]

Essentially there were two main elements in the bill:

(1) Modify the procedures for acquiring communications data and allow this data to be retained.
(2) Transpose EU Directive 2006/24/EC on the retention of communications data into UK law.

In announcing the bill, it was claimed that there were two main benefits of the bill:

1. Communications data plays a key role in counter-terrorism investigations, the prevention and detection of crime and protecting the public. The Bill would bring the

legislative framework on access to communications data up to date with changes taking place in the telecommunications industry and the move to using Internet Protocol (IP) core networks;
2. Unless the legislation is updated to reflect these changes, the ability of public authorities to carry out their crime prevention and public safety duties and to counter these threats will be undermined.[35]

The announcement of the bill – particularly the implications on the fundamental rights and freedoms of individuals – met with immediate criticism. The criticism became more vociferous when it was found out[36] that essentially this Bill was meant to provide legal basis for a £12 billion IT[37] project called the Interception Modernisation Programme (IMP). The objective of the interception modernisation programme is, as stated by the Parliamentary Under-Secretary of State (Lord West of Spithead) in reply to a parliamentary question asked by the Earl of Northesk, 'to maintain the UK's lawful intercept and communications data capabilities in the changing communications environment. It is a cross-government programme, led by the Home Office, to ensure that our capability to lawfully intercept and exploit data when fighting crime and terrorism is not lost.'[38]

Many commentators found that 'The Communications Data Bill changes the rules under which communications details can be retained by the police and security services. In other words, it allows the government to eavesdrop and retain telephone calls, emails and other forms of communications by British citizens to a greater extent than it could before.'[39] The IMP was labelled as the 'überdatabase'.[40]

The two elements of the bill – one part to modify the procedures for acquiring communications data and allow this data to be retained (and allowing for IMP) and the other part to transpose EU Directive 2006/24/EC on the retention of communications data into UK law – have eventually followed two separate paths.

Provisions allowing IMP

The pre-legislative public consultation on the draft Communications Data Bill ended in August 2008. Between July and October 2008, different aspects of the IMP were gradually disclosed (through Parliamentary Questions[41] and interviews.[42] On 20 October 2008 the Information Commissioner's Office called for further consultation as 'it is likely that such a scheme would be a step too far for the British way of life. Creating huge databases containing personal information is never a risk-free option as it is not possible to fully eliminate the danger that the data will fall into the wrong hands. It is therefore of paramount importance that proposals threatening such intrusion into our lives are fully debated.'[43]

By 24 October 2008, the government announced that it was abandoning/postponing the publication of the Communications Data Bill to the next year. The then Home Secretary Jacqui Smith was reported as saying, 'Before proceeding to legislation, I am clear that we need to consult widely with the public and all interested parties to set out the emerging problem, the important capability gaps that we need to address and to look at the possible solutions. . . . We also need to agree what safeguards will be needed, in addition to the many we have in place already, to provide a solid legal framework which protects civil liberties.'[44] Indeed the Communications Data Bill did not make the Queen's Speech in December 2008.[45] In spite of the lack of legal basis, the IMP is still expected to go ahead, even if some have argued that the abandoning of the Data communications bill would slow the progress of the IMP.[46]

Communications data consultation, April 2009

In April 2009, the Home Office launched another public consultation on the retention of communications data (and the Interception Modernisation Programme) entitled *Protecting the Public in a changing Communications Environment*.[47] Conscious of the public resistance towards the creation of an 'überdatabase', in this consultation the government rules out the option of creating a central database to collect and hold communications data.[48] Instead the consultation proposes 'a middle way' requiring communications service providers to collect data identified by legislation as being needed by public authorities (which would include additional data to that collected for their business needs) and to process third part communications data and match it with their own business data.[49]

The consultation was at once welcomed and criticised. Civil rights organisations such as Liberty welcomed the 'climb-down on centralised communications database'.[50] Other groups while acknowledging that ruling out a centralised communications database is a positive step forward, have two main contentions: first, they argue that the proposed 'middle way' presented in the Consultation paper 'is a thinly-disguised outsourced version of a massive state-owned database'.[51] In contrast, some have argued that it is preferable to have the private sector responsible for the personal information, as arguably the private sector has a better reputation at securing personal information than government.[52]

Second, they argue that new technologies (and the uses of new technologies) actually make the distinction of content and communications data very difficult, and hence the government's claim that the retention being sought involves only communications data (and not content) 'is spurious'.[53] As a briefing from the London School of Economics and Political Science points out 'There are increasingly practical difficulties within the new technologies in distinguishing communications data from content although the Home Office's proposed framework of the law is still attempting to do so. In particular the authorisations to request communications data and to intercept content are entirely separate regimes – which law enforcement agencies, Internet Service Providers, telecommunications companies and ultimately the courts have to negotiate and interpret.'[54] In essence the framework dramatically increases surveillance powers without appropriate safeguards to protect citizens' rights to privacy.

The ICO noted further that even communications records alone 'can be highly intrusive even if no content is collected' and the whole process of collecting personal data needs to be 'tightly defined and minimise the level of intrusion with appropriate safeguards in place'.[55]

Where does purpose-specification stand in this debate?

Communications data are initially collected and processed as part of the business practices of any Internet service provider. Following a long standing memorandum of understanding and more recently on the basis of the EU Data Retention Directive (see next section), communications data processed for business purposes are also retained for other purposes, namely for use by law enforcement agencies and other public authorities authorised under the Regulation of Investigatory Powers Act 2000 (RIPA) to use this information. RIPA, Part 1, Chapter II (and associated statutory instruments) list the statutory purposes for which communications data may be accessed. The Communications data consultation does not specifically add new purposes to those already found in RIPA. Yet arguably, if the claim put forward by critics that technically speaking the separation of communications data and content is no longer viable, then the purposes in RIPA are being extended also to content. Similar to the situation of clause 152 (discussed earlier in the paper), this seems to

be another situation where the purpose-specification principle may be being overridden by the government allowing for a wide and relatively unrestricted collection and retention of personal.

One question that arises here is whether the intrusion into citizens' private life that comes with retaining communications data (and content) is a proportionate measure in a democratic society. To some extent the answer to the question can only be answered when a bill with the legal provisions is presented to Parliament. It is at that stage that one can determine whether the limits on what additional information should be retained by communications service providers together with the wide purposes provided for by RIPA sufficiently safeguard fundament rights of citizens. Indeed one question in the Communications data consultation[56] addresses safeguards and asks whether the safeguards outlined in the consultation are sufficient. The consultation does not add any new safeguards – it relies on the safeguards (such as they are) found in RIPA and the true status of RIPA is central to the debate here.

Ever since it was enacted, RIPA has been criticised on a number of counts, *inter alia*, the convoluted way it is written,[57] its wide reasons allowing for communications data to be acquired and the vast number of authorities allowed to have access to communications data. The massive difficulties with RIPA 2000 were colourfully described as follows during the discussions of the draft Data Retention (EC Directive) Regulations 2009 by the Fourth Delegated Legislation Committee:

> *When the Act was passed in 2000, it applied to nine organisations, such as the police and security services; I believe that now it applies to 800 public bodies, including all councils. One has to question whether that was the original intention back in 2000. We are all familiar with the examples cited in the media of RIPA being used to check whether people live in the catchment area of a school to which their children are applying, and to check whether people are cleaning up after their dogs. Clearly, RIPA has been used in a way that was completely unintended and we do not have the safeguards before us today to provide assurances that that type of abuse will not happen in relation to accessing these data as well.*[58] *... RIPA gives all 474 local councils in England, every NHS trust, every fire service, 139 prisons, the Environment Agency and even Royal Mail, the authority – whether in whole, or in part – to access and use communications data, not just national security services. The number of requests for communications data under RIPA in the year ending 31 December 2007 amounted to 519,260 requests.*[59]

The media publicity reporting how local councils and other public authorities make use of RIPA powers for trivial situations – pushing the widely defined purposes for use of these powers to the limit – has triggered another Consultation process. In April 2009,[60] (a few days earlier than the launching of the Communications data consultation) the Home Office launched: *Regulation of Investigatory Powers Act 2000: Consolidation Orders and Codes of Practice.*[61] One of the aims of this consultation is to review the way public authorities use the techniques (directed surveillance, intrusive surveillance, access to communications data) allowed under the Act. In theory, the consultation is an attempt to 'provide greater clarity on when the use of RIPA techniques is more likely to be proportionate'.[62]

The consultation is suggesting to improve the way public authorities use the techniques given to them by law is by 'raising the rank at which techniques are authorised in local authorities to senior executive, and giving elected councillors a role in overseeing the way RIPA techniques are used'.[63] It also suggests that in some cases certain public authorities should no longer have the power to use certain covert techniques and asks the public to propose whether certain public authorities should remain or should be removed from the RIPA framework. The consultation also suggests changes to the codes of practice which provide

statutory guidance on when and how covert investigative techniques should be authorised, the circumstances in which they should be used, and how they are reviewed and overseen by independent commissioners.[64]

As Liberty[65] and other civil rights organisations have pointed out, the consultation does not go far enough. Seeking to review who can exercise power and when is only part of the solution. What is also in need of review are the actual purposes for which the powers are exercised. At this moment in time, the specific purposes for which communications data,[66] directed surveillance[67] and covert human intelligence sources[68] are:

(1) in the interests of national security;
(2) for the purpose of preventing or detecting crime or preventing disorder;
(3) in the interests of the economic well-being of the UK;
(4) in the interests of public safety;
(5) for the purpose of protecting public health; and
(6) for the purpose of assessing or collecting any tax, duty, levy or other charge payable to a government department.

RIPA provides an extra purpose for communications data only:

(7) for the purpose, in an emergency, of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health.

Further grounds can be specified by an Order made by the Secretary of State.[69] SI No. 1878 of 2006 provides the following additional grounds in relation to communications data:

> Article 2(a) – to assist investigations into alleged miscarriages of justice; and
>
> Article 2(b) – to assist in identifying a person who has died or is unable to identify himself because of a physical or mental condition, other than one resulting from crime, or to obtain information about his next of kin or others connected with him or about the reason for his death or condition.

The specified purposes in which RIPA powers can be granted 'are broad and ill-defined'.[70] These purposes are not defined in the law. While one may argue that since these grounds are the same as those allowed under Article 8(2) of the European Convention of Human Rights than no definition needs to be given at law, recent experiences where an expansive interpretation of the grounds has been followed, such as, government restricting drug-users access to welfare benefits is justified to further the 'economic well-being of the UK',[71] suggests that clear, restrictive definitions are necessary. The grounds in Article 8(2) ECHR (in line with numerous judgements of the European Court of Human Rights such as *Rotaru* v *Romania*[72]) can be exercised only if the tests of necessity and proportionality are satisfied. Given that under RIPA there is no appropriate judicial approval given before powers are exercised and whatever the relevant authority subjectively decides is in the interests of national security or the economic well-being of the UK is what will be used to authorise the surveillance,[73] it is even more important for the law to give better defined purposes when the powers can be used to limit unnecessary and disproportionate use of the powers. Clearer limitations on the use of these grounds could have better met the aim of the RIPA Consultation to 'provide greater clarity on when the use of RIPA techniques is more likely to be proportionate'.[74] This Consultation is a lost opportunity to strength the purpose-specification principle, which is evidently being eroded by wide and broadly defined purposes.

Provisions transposing EU Data Retention Directive

The other leg of the Communications Data Bill – the transposition of the Data Retention Directive – followed a different track. One reason for the different track was triggered by the urgency of having to implement the EU Directive by 15 March 2009. The first part of this EU Directive, regarding landline telephones and mobile phones has already been in force in the UK since October 2007 (*Data Retention (EC Directive) Regulations* SI 2007/2199). Like many other EU countries, the UK had delayed implementing the Internet aspects of the Directive for a further 18 months. In August 2008, the Home Office launched a Consultation process on 'the final phase of the transposition of Directive 2006/24/EC on retaining data generated through electronic communications or public communications networks.' The Home Office claimed that 'This consultation is necessary to ensure the law includes internet access, internet telephone service, and internet mail.'[75] The consultation process closed on 31 October 2008 and the Home Office published a response to the public consultation in February 2009.[76] A draft of the regulations was also published in February 2009. Since the Communications Data Bill was abandoned in October, the draft regulations were presented to Parliament as secondary legislation. It has been argued that 'the decision to use secondary legislation is consistent with the approach which led to the *Data Retention (EC Directive) Regulations* SI 2007/2199'[77] a statement which beggars the question 'Then why was the Government originally proposing to include these measures in primary legislation in the first place?'

The draft Data Retention (EC Directive) Regulations 2009 were discussed by the Fourth Delegated Legislation Committee on 16 March 2009. A number of issues were raised during the discussion:

(1) What is actually to be retained – communications data *v* content. Since the scope of the regulations is only to implement the EU Data Retention Directive, the regulations cover only the retention of communication data and not the content of the communication. 'The specific data covered by the directive are information that is generated or processed by communications providers for their own business purposes, such as billing, network management and fraud prevention. Neither the directive nor the regulations apply to any of the contents of a communication.'[78] It was not clear in the debate whether the IMP would include the retention of the contents of a communication.
(2) To whom do the regulations apply – essentially all 'communications service providers' are bound by these regulations. The Committee debated whether social network providers were also bound by these regulations. The Minister argued that they are not and 'That is one reason why the Government are looking at what we should do about the intercept modernisation programme because there are certain aspects of communications which are not covered by the directive.'[79]
(3) Relationship with RIPA 2000 – While these Regulations regulate only the retention of the communications data, access to this retained information is regulated by RIPA 2000. It was pointed out during the debate that while the then Home Secretary has described the use of RIPA as the 'dustbin Stasi'[80] and had promised to consult on proposed changes to RIPA – On 16 December, the then Home Secretary said: 'Early next year, we will consult on a number of proposed changes to RIPA – and we will look at: revisions to the codes of practice that come under the Act; which public authorities can use RIPA powers; raising the bar for how those powers are authorised, and who authorises their use' – the explanatory

memorandum that was presented together with the Regulations noted that no changes to RIPA were necessary. 'Paragraph D4 on page 21 of the explanatory memorandum says:

> It is important to state that access to communications data is governed by the Regulation of Investigatory Powers Act 2000 (RIPA) and no changes to the safeguards set out in that Act are planned.

Then, if the matter needed any further clarification, paragraph D7 on the same page says:

> We do not propose to alter the statutory mechanisms through which data is accessed.

Finally, if that was not clear enough, paragraph D9 on page 22 makes it even more explicit, by saying: 'We consider that the safeguards set out in RIPA provide a rigorous check against disproportionate interferences with individuals' right to respect of their privacy. The implementation of this Directive does not alter the balance in that debate.'
So, no changes are planned.[81]
At the end of April 2009 (just after the Regulations came into effect) the much awaited RIPA Consultation was launched (as discussed in the earlier section).

(4) Relationship with IMP – It was noted that the relationship between these Regulations and the IMP were still to be clarified. The consultation promised upon the withdrawal of the Communications Data Bill in October 2008 has still to take place and hence the uncertainty continues. The April 2009 Communications Data Consultation does not clarify this relationship either.
(5) Lack of safeguards – the Regulations offer no safeguards for the protection of privacy and fundamental rights as it relies on RIPA – which unfortunately has actually very little safeguards.[82]

The Data Retention (EC Directive) Regulations 2009 Regulations SI 2009/859[83] became law on 2 April 2009 and came into force on 6 April 2009.

Conclusion

It is understandable that in a reality where organised crime is getting consistently more elaborate and organised and the threat of terrorism is ongoing then governments want to build the 'best' means to protect citizens from organised crime and terrorism. It is equally important however that the 'best' means do not ignore other fundamental rights of citizens, the right to a private life without unnecessary interference from public authorities.

All the Bills and Consultations reviewed here make reference to this balancing act between safeguarding security and safeguarding the right to privacy. Yet in reviewing them we come to the conclusion that, more often than not, the balance tilts towards giving wide powers to 'protecting citizen safety'. The very legal tools, more generally found in the Human Rights Act and more specifically in the Data Protection Act, given to the legislator to protect citizens' are not being used. This paper looks at how the purpose-specification principle – the tool provided by the Data Protection Act to limit the use of personal information – is being used in the recent Bills and Consultations. The evidence shows that overall – whether in the data sharing proposals, whether in the Communications Data proposals (and introduction of the Interception Modernisation

Programme), whether in the RIPA Consultation – the purpose-specification principle is being overridden or ignored.

The overriding of the purpose-specification principle comes in various forms: there are instances, such as in RIPA where the purposes established in the law are broad and ill-defined and have in practice been abused of; there are instances where purpose is completely ignored (as if no such principle exists) as in the proposals of Clause 152; and instances where the drafting is so convoluted that it is very difficult to determine what the actual purposes are.

For a variety of reasons, mostly thanks to the mobilisation of civil society and the intervention of politicians ('jumping at times on the band wagon'), the data sharing provisions and the interceptions modernisation programme have been temporarily stopped. One waits now to see the government's reaction to the two consultation processes (on communications data and RIPA) and determine whether the messages sent during the discussions of the data sharing provisions and the communications data have been heard at all.

What is important to note is that by avoiding to take a clear and decisive position on the legality and conditions for data sharing and on the Interception Modernisation Programme, fundamental safeguards of citizens' rights of data protection are being systematically destroyed or ignored.

The authors hold that it is neither doctrinaire nor alarmist to conclude that the non-appearance of law in a timely fashion is a failure of technology law to control use and abuse of technology *vis-à-vis* privacy, human dignity and an emerging *lex personalitatis*. The UK government has not satisfactorily reassured the public or its critics that it will have adequate legal safeguards in place *before* it goes ahead with intrusive measures under the IMP and some have alleged that work on the programme is still moving forward with anything between £1 billion and £2 billion pounds having been made available for the next phase of investment in the scheme. The up-coming 2010 election and other concerns seem to have diverted attention from the pressing need of action on this front. In November 2009 the Home Office confirmed that 'Plans to store information about every phone call, email and internet visit in the United Kingdom ... been delayed until after the election amid protests that it would be intrusive and open to abuse'.[84] For the second year in succession the UK government left the IMP out of the Queen's speech in November 2009 and it is clear that, as the 2010 election looms ever closer, it does not wish to have a re-run of anything as contentious as the January–March 2009 debate on the Justice and Coroner's Bill. Doubtless, the legislative saga is now set to continue some time after May 2010 and respect for the principle of purpose will be re-examined again then. Whether the security services and their technologists will have downed IMP-related tools while the politicians focus on other priorities will remain anybody's guess.

Notes

1. In the Data Protection Act 1998, the purpose-specification principle is the second Data Protection Principle, which states that 'Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.' Data Protection Act 1998 Schedule 1, Part 1, 2.
2. Robert Gellman, 'Privacy: Finding a Balanced Approach to Consumer Options'. Available at http://www.cdt.org/privacy/ccp/consentchoice4.pdf
3. London School of Economics and Political Science, 'The Identity Project: An Assessment of the UK Identity Cards Bill & Its Implications', 27 June 2005 at p. 26, available at http://is2.lse.ac.uk/IDcard/identityreport.pdf
4. Joseph A. Cannataci, '*Lex Personalitatis* and Technology-driven Law', *SCRIPTed* 5, no, 1 (2008): 1, available at http://www.law.ed.ac.uk/ahrc/script-ed/vol5-1/editorial.asp

5. Richard Thomas and Mark Walport, 'Data Sharing Review Report' (2008), available at http://www.justice.gov.uk/docs/data-sharing-review-report.pdf
6. See in particular, ibid., 46–48.
7. Ibid., 39.
8. Ibid.
9. Ibid., 2.
10. UK Ministry of Justice, Response to Data Sharing Review Report, November 2008, available at http://www.justice.gov.uk/publications/docs/response-data-sharing-review.pdf
11. Ibid., p. 16.
12. Coroners and Justice Bill 2009, Section 152, introducing a new section 50A(4) to the Data Protection Act 1998.
13. Coroners and Justice Bill 2009, Section 152, introducing a new section 50A(1) to the Data Protection Act 1998.
14. See note 12 above.
15. J. Cannataci and J.P. Mifsud Bonnici, 'The UK 2007 Data Protection Fiasco: Moving On From Bad Policy And Bad Law', *International Review of Law, Computers and Technology*, 23, nos. 1–2 (2009): 47–76
16. Sally Almandras, Sally Broadbridge, Grahame Danby and Pat Strickland, 'The Coroners & Justice Bill: Crime & Data Protection, Bill 9 of 2008-09', Research Paper 09/06, House of Commons Library, 22 January 2006, at p. 108
17. Coroners and Justice Bill 2009, Clause 152 introducing a new section 50A(3) to the Data Protection Act 1998.
18. Information Commissioner Response to the Joint Committee of Human Rights, 27 February 2009, available at http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/jchr_memorandum_letter_270209.pdf
19. Ibid.
20. Bold is found in the original. See Information Commissioner, Memorandum submitted by the Information Commissioner to the Public Bill Committee (30 January 2009), available at http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/cj_bill_ic_memorandum_300109.pdf
21. See for example report in Out-Law, 'Government Data Sharing Plan Could Extend to the Private Sector', 16 January 2009, available at http://www.out-law.com/page-9716
22. Ibid.
23. See Zosia Kmietowicz, 'Government Removes Data Sharing Clause from Coroners Bill', *British Medical Journal* 338 (11 March 2009): b1009.
24. Committee stage discussions on 26 February 2009, available at http://www.publications.parliament.uk/pa/cm200809/cmpublic/coroners/090226/pm/90226s06.htm
25. Ibid.
26. Amendments to Coroners and Justice Bill Thursday 26 February 2009, available at http://www.publications.parliament.uk/pa/cm200809/cmpublic/coroners/090226/pm/90226s01.htm
27. Speech of Mr Bellingham, available at http://www.publications.parliament.uk/pa/cm200809/cmpublic/coroners/090226/pm/90226s02.htm
28. Bold in original. Human Rights Joint Committee–Eighth Report- Legislative Scrutiny: Coroners and Justice Bill, available at http://www.publications.parliament.uk/pa/jt200809/jtselect/jtrights/57/5706.htm
29. See note 26.
30. Ibid.
31. Committee stage discussions on 26 February 2009, available at http://www.publications.parliament.uk/pa/cm200809/cmpublic/coroners/090226/pm/90226s06.htm#end
32. David Barrett, 'Government Abandons Data-Sharing Scheme', *The Telegraph*, 7 March 2009. Available at http://www.telegraph.co.uk/news/newstopics/politics/lawandorder/4954058/Government-abandons-data-sharing-scheme.html
33. David Leppard, 'There's No Hiding Place as Spy HQ Plans to See All', *The Times*, 5 October 2008, available at http://www.timesonline.co.uk/tol/news/uk/article4882622.ece
34. See Leader of the House of Commons, 'Introduction to Communications Data Bill', available at http://www.commonsleader.gov.uk/output/page2466.asp?p=1&g=59FD1FD3-8251-4783-B40B-C6702020AA70 and available at http://www.official-documents.gov.uk/document/cm73/7372/7372.pdf

35. Ibid.
36. In a *Times* article: Richard Ford, 'Big Brother' Database for Phones and Emails', *The Times*, 20 May 2008, available at http://business.timesonline.co.uk/tol/business/industry_sectors/telecoms/article3965033.ece
37. See Chris Williams, 'Spy Chiefs Plot £12bn IT Spree for Comms Uber database: Black Boxes to keep Black's Firm in the Black', 7 October 2008, available at http://www.theregister.co.uk/2008/10/07/detica_interception_modernisation/
38. Hansard 8 July 2008: Column WA73, available at http://www.publications.parliament.uk/pa/ld200708/ldhansrd/text/80708w0001.htm
39. 'Communications Date Bill', 16 October 2008, available at http://www.politics.co.uk/legislation/legal-and-constitutional/communications-data-bill-$1245133.htm
40. Chris Williams op. cit.
41. 9 June 2008. Dr Julian Lewis:asked on measures planned for the comprehensive storage of national telephone and e-mail communications data. Available at http://www.parliament.uk/commons/lib/research/briefings/snha-04884.pdf
    8 July 2008. Lord Northesk: asked on objectives of IMP, financing and cost. Available at http://www.publications.parliament.uk/pa/ld200708/ldhansrd/text/80708w0001.htm
    July 2008. Baroness Miller of Chilthorne Domer: asked on what guidance had been given to Internet Service Providers on when and how they can intercept their customers' website use; and what information they have made available to the public about the privacy issues involved, available at http://www.parliament.uk/commons/lib/research/briefings/snha-04884.pdf
    July 2008. Viscount Bridgeman: asked whether the government would withdraw their plans for a communications data Bill to set up a database logging every private phone call and e-mail following the opposition to the idea, available at http://www.parliament.uk/commons/lib/research/briefings/snha-04884.pdf
42. See, for example, Leppard, 'There's No Hiding Place'; Williams, 'Spy chiefs Plot £12bn IT Spree'.
43. Information Commissioner's Office, ICO Statement on the Communications Data Bill, 20 October 2008. Available at http://www.ico.gov.uk/upload/documents/pressreleases/2008/ico_statement_comms_data_bill.pdf
44. Ian Grant, 'Government Scraps Communications Data Bill', 24 October 2008. Available at http://www.computerweekly.com/Articles/2008/10/24/232819/government-scraps-communications-data-bill.htm
45. Karl Flinders, £12bn Snooping Database Ommitted from Queen's Speech, 3 December 2008. Available at http://www.computerweekly.com/Articles/2008/12/03/233713/12bn-snooping-database-ommitted-from-queens-speech.htm
46. Ibid.
47. UK Home Office, 'Protecting the Public in a Changing Communications Environment', April 2009 (Ref.: Cmmd. 7586), available at http://www.homeoffice.gov.uk/documents/cons-2009-communications-data. The Consultation process ended on 20 July 2009. No official response by government had been published by the time this paper was submitted for review.
48. Speech of then Home Secretary while presenting the Consultation paper to the house on 27 April 2009, available at http://www.publications.parliament.uk/pa/cm200809/cmhansrd/cm090427/wmstext/90427m0002.htm
49. UK Home Office, 'Protecting the Public' at p. 4, para. 19.
50. See Liberty Press Release, 'Liberty Welcomes Government Climb-Down on Centralised Communications Database', 27 April 2009, available at http://www.liberty-human-rights.org.uk/news-and-events/1-press-releases/2009/27-04-09-liberty-welcomes-government-climb-down-on-centralised-communicati.shtml
51. Letter by Andrew Findlay in response to Consultation (date 30 April 2008), available at http://www.skills-1st.co.uk/papers/policy/commsdata-200904.pdf
52. Marc Dautlich, head of the data protection group at Olswang, 'I trust the private sector more than I trust the government, based on the number of recent breaches. Plus the private sector is regulated and has its public reputation to think about.' As reported in James Boxell, 'Smith Drops Plans for State Web Database', *Financial Times Online*, 28 April 2009, available at http://www.ft.com/cms/s/0/070ca8e0-3382-11de-8f1b-00144feabdc0.html?ftcamp=rss&nclick_check=1

53. See No2ID Press Release, 'Jacqui Smith Announces UK to Have Most Intrusive Surveillance Powers Anywhere', 27 April 2009, available at http://www.no2id.net/news/pressRelease/release.php?name=Smith_announces
54. The London School of Economics and Political Science, 'Briefing on the Interception Modernisation Programme', 2009, available at http://www.lse.ac.uk/collections/informationSystems/research/policyEngagement/IMP_Briefing.pdf
55. See Information Commissioner's statement on the Communications Data Bill, date 27 April 2009, available at http://www.ico.gov.uk/upload/documents/pressreleases/2009/ico_statement_dc_bill.pdf
56. The Consultation asks the public to comment on four questions:

    Q1. On the basis of this evidence and subject to current safeguards and oversight arrangements, do you agree that communications data is vital for law enforcement, security and intelligence agencies and emergency services in tackling serious crime, preventing terrorism and protection the public?

    Q2. Is it right for government to maintain this capability by responding to the new communications environment?

    Q3. Do you support the government's approach to maintaining our capabilities? Which of the solutions should it adopt?

    Q4. Do you believe that the safeguards outlined are sufficient for communications data in the future?

    UK Home Office, 'Communications Data Consultation', 27 April 2009, available at http://press.homeoffice.gov.uk/speeches/comms-data-consultation.html

57. The Court of Appeal has labelled it 'a particularly puzzling statute' in *R* v. *W* [2003] EWCA Crim 1632; [2003] 1 WLR 2902, 12 June 2003, at para 98.
58. Transcript of debate of Fourth Delegated Legislation Committee held 16 March 2009, available at http://www.publications.parliament.uk/pa/cm200809/cmgeneral/deleg4/090316/90316s01.htm
59. Transcript of debate of Fourth Delegated Legislation Committee held 16 March 2009, available at http://www.publications.parliament.uk/pa/cm200809/cmgeneral/deleg4/090316/90316s01.htm#end
60. The Consultation process ended on 10 July 2009. No official response by government had been published by the time this paper was submitted for review at the end of July 2009.
61. UK Home Office, 'Regulation of Investigatory Powers Act 2000: Consolidating Orders and Codes of Practice – Consultation and response', available at http://www.homeoffice.gov.uk/documents/cons-2009-ripa
62. Regulation of Investigatory Powers Act 2000: Consolidating Orders and Codes of Practice (April 2009) at p. 4, available at http://www.homeoffice.gov.uk/documents/cons-2009-ripa
63. Ibid., p. 6.
64. Ibid., p. 7.
65. See Liberty, 'Liberty's Response to the Home Office Consultation on the Regulation of Investigatory Powers Act 2000: Consolidating Orders and Codes of Practice' (2009), at p. 24, available at http://www.liberty-human-rights.org.uk/pdfs/policy-09/liberty-s-response-to-the-ripa-consultation.pdf
66. Section 22 RIPA.
67. Section 28 RIPA.
68. Section 29 RIPA.
69. See sections 22(h) (communications data), 28(g) (directed surveillance) and 29(g) (covert human intelligence sources).
70. Liberty, 'Liberty's Response to the Home Office', p. 13.
71. See the Explanatory Notes to the Welfare Reform Bill at paragraph 418, available at: http://www.publications.parliament.uk/pa/cm200809/cmbills/008/en/2009008en.pdf as reported in Liberty, 'Liberty's Response to the Home Office', p. 14.
72. Grand Chamber decision 2000 (Application 28341/95).
73. Liberty, 'Liberty's Response to the Home Office', p. 14.
74. Regulation of Investigatory Powers Act 2000, p. 4

75. UK Home Office, 'Consultation: Transposition of Directive 2006/24/EC', available at http://www.homeoffice.gov.uk/documents/cons-2008-transposition-dir/
76. Government Response to the Public Consultation on the Transposition of Directive 2006/24/EC – February 2009, available at http://www.homeoffice.gov.uk/documents/cons-2008-transposition-dir/cons-2008-transposition-response?view=Binary
77. Grahame Danby, 'House of Commons Library Standard Note No. SN/HA/4884 on the Draft Communications Data Bill', January 2009, available at http://www.parliament.uk/commons/lib/research/briefings/snha-04884.pdf
78. The Minister for Security, Counter-Terrorism, Crime and Policing (Mr Vernon Coaker) in transcript of debate of Fourth Delegated Legislation Committee held 16 March 2009, available at http://www.publications.parliament.uk/pa/cm200809/cmgeneral/deleg4/090316/90316s01.htm
79. The Minister for Security, Counter-Terrorism, Crime and Policing (Mr Vernon Coaker) in transcript of debate of Fourth Delegated Legislation Committee held 16 March 2009, available at http://www.publications.parliament.uk/pa/cm200809/cmgeneral/deleg4/090316/90316s01.htm
80. Home Secretary Jacqui Smith Speech 'Protecting Rights, Protecting Society' delivered to the Intellect Trade Association on 16 December 2008, available at http://press.homeoffice.gov.uk/Speeches/home-sec-protecting-rights
81. Transcript of debate of Fourth Delegated Legislation Committee held 16 March 2009, available at http://www.publications.parliament.uk/pa/cm200809/cmgeneral/deleg4/090316/90316s01.htm and Explanatory Memorandum, available at http://www.opsi.gov.uk/si/si2009/draft/em/ukdsiem_9780111473894_en.pdf
82. Transcript of debate of Fourth Delegated Legislation Committee held 16 March 2009. See previous note.
83. Statutory Instrument 2009 No. 859 Electronic Communications: The Data Retention (EC Directive) Regulations 2009', available at http://www.opsi.gov.uk/si/si2009/pdf/uksi_20090859_en.pdf
84. Nigel Morris and Robert Verkaik, 'Ministers Cancel "Big Brother" Database', *The Independent*, 10 November 2009.

10/31/2010

Appendix Five

Data Protection Vision 2020

options for improving European policy and legislation during 2010-2020

Joseph A. Cannataci

The United States Mission to the European Union

http://useu.usmission.gov *Brussels, Belgium*

U.S., EU Reach Agreement on Common Personal Data Protection Principles

October 28, 2009

The joint statement adopted at the October 28, 2009, United States-European Union Justice and Home Affairs Ministerial acknowledged the completion of the High Level Contact Group's (HLCG) common principles to protect personal data. The common principles, consolidated into one document based on the HLCG's May 2008 and October 2009 reports, are below.

The United States looks forward to the negotiation of a binding international EU-U.S. agreement embodying the principles, which would serve as a solid basis for our law enforcement authorities for even further enhanced cooperation, while ensuring the availability of full protection for our citizens.

Below is the text of the common principles to on privacy and personal data protection:

Principles on Privacy and Personal Data Protection for Law Enforcement Purposes for which common language has been developed (common principles)

The European Union would apply these principles for 'law enforcement purposes' meaning use for the prevention, detection, investigation, or prosecution of any criminal offense.

The United States would apply these principles for 'law enforcement purpose,' meaning use for the prevention, detection, suppression, investigation, or prosecution of any criminal offense or violation of law related to border enforcement, public security, and national security, as well as for non-criminal judicial or administrative proceedings related directly to such offenses or violations.

1. Purpose Specification/Purpose Limitation.

Personal information [should/shall] be processed for specific legitimate law enforcement purposes in accordance with the law and subsequently processed only insofar as this is not incompatible with the law enforcement purpose of the original collection of the personal information.

2. Integrity/Data Quality.

Personal information should be maintained with such accuracy, relevance, timeliness and completeness as is necessary for lawful processing.

3. Relevant and Necessary/Proportionality.

Personal information may only be processed to the extent it is relevant, necessary and appropriate to accomplish a law enforcement purpose laid down by law.

4. Information Security.

Personal information must be protected by all appropriate technical, security and organizational procedures and measures to guard against such risks as loss; corruption; misuse; unauthorized access, alteration, disclosure or destruction; or any other risks to the security, confidentially or integrity of the information. Only authorized individuals with an identified purpose may have access to personal information.

5. Special Categories of Personal Information.

Personal information revealing racial or ethnic origins, political opinions or religious or philosophical beliefs, or trade union membership, as well as personal information concerning health or sexual life or other categories defined under domestic law may not be processed unless domestic law provides appropriate safeguards.

6. Accountability.

Public entities processing personal information [shall/should] be accountable for complying with domestic law and rules and on the protection of personal information.

7. Independent and Effective Oversight.

A system of independent and effective data protection supervision [shall/should] exist in the form of a public supervisory authority with effective powers of intervention and enforcement. These responsibilities may be carried out by a specialized public data protection authority or by more than one supervisory public authority to meet the particular circumstances of different legal systems.

8. Individual Access and Rectification.

[An/every] individual [should/shall] be provided with access to and the means to seek rectification and/or expungement of his or her personal information. In appropriate cases, an individual may object to processing of personal information related to him or her.

9. Transparency and Notice.

An individual [should/shall] be informed, as required by law, with general and individual notice at least as to the purpose of processing of personal information concerning him or her and who will be processing that information, under what rules or laws, the types of third parties to whom information is disclosed as well as other information insofar as is necessary to ensure fairness including rights and remedies available to the individual.

10. Redress

Recognizing that both the US and EU provide multiple mechanisms for administrative and judicial redress, wherever an individual's privacy has been infringed or data protection rules have been violated with respect to that individual, that individual [should/shall] have, before an impartial competent authority, independent court or tribunal, an effective remedy and/or appropriate and effective sanctions.

11. Automated Individual Decisions.

Decisions producing significant adverse actions concerning the relevant interests of the individual may not be based solely on the automated processing of personal information without human involvement unless provided for by domestic law and with appropriate safeguards in place, including the possibility to obtain human intervention.

12. Restrictions on onward transfers to third countries.

Where personal information is transmitted or made available by a competent authority of the sending country or by private parties in accordance with the domestic law of the sending country to a competent authority of the receiving country, the competent authority of the receiving country may only authorise or carry out an onward transfer of this information to a competent authority of a third country if permitted under its domestic law and in accordance with existing applicable international agreements and international arrangements between the sending and receiving country. In the absence of such international agreements and international arrangements, such transfers should moreover support legitimate public interests consisting of: national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences, breaches of ethics of regulated professions, or the protection of the data subject. In all cases transfers should be fully consistent with these common principles, especially the limitation/purpose specification.

Issues pertinent to the transatlantic relationship

On private entities' obligations, any adverse impact on private entities resulting from data transfers, including those impacts deriving from diverging legal and regulatory requirements, should be avoided to the greatest extent possible.

On preventing undue impact on relations with third countries, when the European Union or the United States has international agreements or arrangements for information sharing with third countries, each should use their best endeavors to avoid putting those third countries in a difficult position because of differences relating to data privacy including legal and regulatory requirements.

On specific agreements relating to information exchanges and privacy and personal data protection, when the European Union and the United States agree that a clear legal necessity arises in particular due to a serious conflict of laws substantiated by one party, the processing of personal information in specific areas should be made subject to specific conditions and should include the necessary safeguards for the protection of privacy and personal data and individual liberties through the negotiation of an information sharing agreement. Such rules may offer individuals a wider measure of protection.

On issues related to the institutional framework of the EU and the U.S., the European Union and the United States intend to consult each other as necessary to discuss and if possible resolve matters arising from divergent legal and regulatory requirements.

On equivalent and reciprocal application of data privacy law, the European Union and the United States should use best efforts to ensure respect for the requirements, taken as a whole as opposed to singular examples, that each asks the other to observe.

-

10/31/2010

Appendix Six

Data Protection Vision 2020

options for improving European policy and legislation during 2010-2020

Joseph A. Cannataci

III

(Acts adopted under the EU Treaty)

ACTS ADOPTED UNDER TITLE VI OF THE EU TREATY

COUNCIL FRAMEWORK DECISION 2008/977/JHA

of 27 November 2008

on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on European Union, and in particular Articles 30, 31 and 34(2)(b) thereof,

Having regard to the proposal from the Commission,

Having regard to the opinion of the European Parliament [1],

Whereas:

(1) The European Union has set itself the objective of maintaining and developing the Union as an area of freedom, security and justice in which a high level of safety is to be provided by common action among the Member States in the fields of police and judicial cooperation in criminal matters.

(2) Common action in the field of police cooperation under Article 30(1)(b) of the Treaty on European Union and common action on judicial cooperation in criminal matters under Article 31(1)(a) of the Treaty on European Union imply a need to process the relevant information which should be subject to appropriate provisions on the protection of personal data.

(3) Legislation falling within the scope of Title VI of the Treaty on European Union should foster police and judicial cooperation in criminal matters with regard to its efficiency as well as its legitimacy and compliance with fundamental rights, in particular the right to privacy and to the protection of personal data. Common standards regarding the processing and protection of personal data processed for the purpose of preventing and combating crime contribute to the achieving of both aims.

(4) The Hague Programme on strengthening freedom, security and justice in the European Union, adopted by the European Council on 4 November 2004, stressed the need for an innovative approach to the cross-border exchange of law-enforcement information under the strict observation of key conditions in the area of data protection and invited the Commission to submit proposals in this regard by the end of 2005 at the latest. This was reflected in the Council and Commission Action Plan implementing the Hague Programme on strengthening freedom, security and justice in the European Union [2].

(5) The exchange of personal data within the framework of police and judicial cooperation in criminal matters, notably under the principle of availability of information as laid down in the Hague Programme, should be supported by clear rules enhancing mutual trust between the competent authorities and ensuring that the relevant information is protected in a way that excludes any discrimination in respect of such cooperation between the Member States while fully respecting fundamental rights of individuals. Existing instruments at the European level do not suffice; 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 [3] does not apply to the processing of personal data in the course of an activity which falls outside the scope of Community law, such as those provided for by Title VI of the Treaty on European Union, nor, in any case, to processing operations concerning public security, defence, state security or the activities of the State in areas of criminal law.

[1] OJ C 125 E, 22.5.2008, p. 154.

[2] OJ C 198, 12.8.2005, p. 1.

[3] OJ L 281, 23.11.1995, p. 31.

(6) This Framework Decision applies only to data gathered or processed by competent authorities for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. This Framework Decision should leave it to Member States to determine more precisely at national level which other purposes are to be considered as incompatible with the purpose for which the personal data were originally collected. In general, further processing for historical, statistical or scientific purposes should not be considered as incompatible with the original purpose of the processing.

(7) The scope of this Framework Decision is limited to the processing of personal data transmitted or made available between Member States. No conclusions should be inferred from this limitation regarding the competence of the Union to adopt acts relating to the collection and processing of personal data at national level or the expediency for the Union to do so in the future.

(8) In order to facilitate data exchanges within the Union, Member States intend to ensure that the standard of data protection achieved in national data processing matches that provided for in this Framework Decision. With regard to national data processing, this Framework Decision does not preclude Member States from providing safeguards for the protection of personal data higher than those established in this Framework Decision.

(9) This Framework Decision should not apply to personal data which a Member State has obtained within the scope of this Framework Decision and which originated in that Member State.

(10) The approximation of Member States' laws should not result in any lessening of the data protection they afford but should, on the contrary, seek to ensure a high level of protection within the Union.

(11) It is necessary to specify the objectives of data protection within the framework of police and judicial activities and to lay down rules concerning the lawfulness of processing of personal data in order to ensure that any information that might be exchanged has been processed lawfully and in accordance with fundamental principles relating to data quality. At the same time the legitimate activities of the police, customs, judicial and other competent authorities should not be jeopardised in any way.

(12) The principle of accuracy of data is to be applied taking account of the nature and purpose of the processing concerned. For example, in particular in judicial proceedings data are based on the subjective perception of individuals and in some cases are totally unverifiable. Consequently, the requirement of accuracy cannot appertain to the accuracy of a statement but merely to the fact that a specific statement has been made.

(13) Archiving in a separate data set should be permissible only if the data are no longer required and used for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. Archiving in a separate data set should also be permissible if the archived data are stored in a database with other data in such a way that they can no longer be used for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. The appropriateness of the archiving period should depend on the purposes of archiving and the legitimate interests of the data subjects. In the case of archiving for historical purposes a very long period may be envisaged.

(14) Data may also be erased by destroying the data medium.

(15) As regards inaccurate, incomplete or no longer up-to-date data transmitted or made available to another Member State and further processed by quasi-judicial authorities, meaning authorities with powers to make legally binding decisions, its rectification, erasure or blocking should be carried out in accordance with national law.

(16) Ensuring a high level of protection of the personal data of individuals requires common provisions to determine the lawfulness and the quality of data processed by competent authorities in other Member States.

(17) It is appropriate to lay down at the European level the conditions under which competent authorities of the Member States should be allowed to transmit and make available personal data received from other Member States to authorities and private parties in Member States. In many cases the transmission of personal data by the judiciary, police or customs to private parties is necessary to prosecute crime or to prevent an immediate and serious threat to public security or to prevent serious harm to the rights of individuals, for example, by issuing alerts concerning forgeries of securities to banks and credit institutions, or, in the area of vehicle crime, by communicating personal data to insurance companies in order to prevent illicit trafficking in stolen motor vehicles or to improve the conditions for the recovery of stolen motor vehicles from abroad. This is not tantamount to the transfer of police or judicial tasks to private parties.

(18) The rules in this Framework Decision regarding the transmission of personal data by the judiciary, police or customs to private parties do not apply to the disclosure of data to private parties (such as defence lawyers and victims) in the context of criminal proceedings.

(19) The further processing of personal data received from, or made available by, the competent authority of another Member State, in particular the further transmission of or making available such data, should be subject to common rules at European level.

(20) Where personal data may be further processed after the Member State from which the data were obtained has given its consent, each Member State should be able to determine the modalities of such consent, including, for example, by means of a general consent for categories of information or categories of further processing.

(21) Where personal data may be further processed for administrative proceedings, these proceedings also include activities by regulatory and supervisory bodies.

(22) The legitimate activities of the police, customs, judicial and other competent authorities may require that data are sent to authorities in third States or international bodies that have obligations for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

(23) Where personal data are transferred from a Member State to third States or international bodies, these data should, in principle, benefit from an adequate level of protection.

(24) Where personal data are transferred from a Member State to third States or international bodies, such transfer should, in principle, take place only after the Member State from which the data were obtained has given its consent to the transfer. Each Member State should be able to determine the modalities of such consent, including, for example, by means of a general consent for categories of information or for specified third States.

(25) The interests of efficient law enforcement cooperation require that where the nature of a threat to the public security of a Member State or a third State is so immediate as to render it impossible to obtain prior consent in good time, the competent authority should be able to transfer the relevant personal data to the third State concerned without such prior consent. The same could apply where other essential interests of a Member State of equal importance are at stake, for example where the critical infrastructure of a Member State could be the subject of an immediate and serious threat or where a Member State's financial system could be seriously disrupted.

(26) It may be necessary to inform data subjects regarding the processing of their data, in particular where there has been particularly serious encroachment on their rights as a result of secret data collection measures, in order to ensure that data subjects can have effective legal protection.

(27) Member States should ensure that the data subject is informed that the personal data could be or are being collected, processed or transmitted to another Member State for the purpose of prevention, investigation, detection, and prosecution of criminal offences or the execution of criminal penalties. The modalities of the right of the data subject to be informed and the exceptions thereto should be determined by national law. This may take a general form, for example, through the law or through the publication of a list of the processing operations.

(28) In order to ensure the protection of personal data without jeopardising the interests of criminal investigations, it is necessary to define the rights of the data subject.

(29) Some Member States have provided for the right of access of the data subject in criminal matters through a system where the national supervisory authority, in place of the data subject, has access to all the personal data related to the data subject without any restriction and may also rectify, erase or update inaccurate data. In such a case of indirect access, the national law of those Member States may provide that the national supervisory authority will inform the data subject only that all the necessary verifications have taken place. However, those Member States also provide for possibilities of direct access for the data subject in specific cases, such as access to judicial records, in order to obtain copies of own criminal records or of documents relating to own hearings by the police services.

(30) It is appropriate to establish common rules on confidentiality and security of processing, on liability and penalties for unlawful use by competent authorities and on judicial remedies available to the data subject. It is, however, for each Member State to determine the nature of its tort rules and of the penalties applicable to violations of domestic data protection provisions.

(31) This Framework Decision allows the principle of public access to official documents to be taken into account when implementing the principles set out in this Framework Decision.

(32) When necessary to protect personal data in relation to processing which by scale or by type holds specific risks for fundamental rights and freedoms, for example processing by means of new technologies, mechanisms or procedures, it is appropriate to ensure that the competent national supervisory authorities are consulted prior to the establishment of filing systems aimed at the processing of these data.

(33) The establishment in Member States of supervisory authorities, exercising their functions with complete independence, is an essential component of the protection of personal data processed within the framework of police and judicial cooperation between the Member States.

(34) The supervisory authorities already established in Member States under Directive 95/46/EC should also be able to assume responsibility for the tasks to be performed by the national supervisory authorities to be established under this Framework Decision.

(35) Such supervisory authorities should have the necessary means to perform their duties, including powers of investigation and intervention, particularly in cases of complaints from individuals, or powers to engage in legal proceedings. These supervisory authorities should help to ensure transparency of processing in the Member States within whose jurisdiction they fall. However, their powers should not interfere with specific rules set out for criminal proceedings or the independence of the judiciary.

(36) Article 47 of the Treaty on European Union stipulates that nothing in it is to affect the Treaties establishing the European Communities or the subsequent Treaties and Acts modifying or supplementing them. Accordingly, this Framework Decision does not affect the protection of personal data under Community law, in particular as provided for in Directive 95/46/EC, in Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data [1] and in Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2].

(37) This Framework Decision is without prejudice to the rules pertaining to illicit access to data laid down in Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems [3].

(38) This Framework Decision is without prejudice to existing obligations and commitments incumbent upon Member States or upon the Union by virtue of bilateral and/or multilateral agreements with third States. Future agreements should comply with the rules on exchanges with third States.

(39) Several acts, adopted on the basis of Title VI of the Treaty on European Union, contain specific provisions on the protection of personal data exchanged or otherwise processed pursuant to those acts. In some cases these provisions constitute a complete and coherent set of rules covering all relevant aspects of data protection (principles of data quality, rules on data security, regulation of the rights and safeguards of data subjects, organisation of supervision and liability) and they regulate these matters in more detail than this Framework Decision. The relevant set of data protection provisions of those acts, in particular those governing the functioning of Europol, Eurojust, the Schengen Information System (SIS) and the Customs Information System (CIS), as well as those introducing direct access for the authorities of Member States to certain data systems of other Member States, should not be affected by this Framework Decision. The same applies in respect of the data protection provisions governing the automated transfer between Member States of DNA profiles, dactyloscopic data and national vehicle registration data pursuant to the Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime [4].

(40) In other cases the provisions on data protection in acts, adopted on the basis of Title VI of the Treaty on European Union, are more limited in scope. They often set specific conditions for the Member State receiving information containing personal data from other Member States as to the purposes for which it can use those data, but refer for other aspects of data protection to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981 or to national law. To the extent that the provisions of those acts imposing conditions on receiving Member States as to the use or further transfer of personal data are more restrictive than those contained in the corresponding provisions of this Framework Decision, the former provisions should remain unaffected. However, for all other aspects the rules set out in this Framework Decision should be applied.

(41) This Framework Decision does not affect the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, the Additional Protocol to that Convention of 8 November 2001 or the Council of Europe conventions on judicial cooperation in criminal matters.

[1] OJ L 8, 12.1.2001, p. 1.
[2] OJ L 201, 31.7.2002, p. 37.
[3] OJ L 69, 16.3.2005, p. 67.
[4] OJ L 210, 6.8.2008, p. 1.

(42) Since the objective of this Framework Decision, namely the determination of common rules for the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, cannot be sufficiently achieved by the Member States, and can therefore, by reason of the scale and effects of the action, be better achieved at the Union level, the Union may adopt measures in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty establishing the European Community and referred to in Article 2 of the Treaty on European Union. In accordance with the principle of proportionality as set out in Article 5 of the Treaty establishing the European Community, this Framework Decision does not go beyond what is necessary to achieve that objective.

(43) The United Kingdom is taking part in this Framework Decision, in accordance with Article 5 of the Protocol integrating the Schengen *acquis* into the framework of the European Union annexed to the Treaty on European Union and to the Treaty establishing the European Community, and Article 8(2) of Council Decision 2000/365/EC of 29 May 2000 concerning the request of the United Kingdom of Great Britain and Northern Ireland to take part in some of the provisions of the Schengen *acquis* ([1]).

(44) Ireland is taking part in this Framework Decision in accordance with Article 5 of the Protocol integrating the Schengen *acquis* into the framework of the European Union annexed to the Treaty on European Union and to the Treaty establishing the European Community, and Article 6(2) of Council Decision 2002/192/EC of 28 February 2002 concerning Ireland's request to take part in some of the provisions of the Schengen *acquis* ([2]).

(45) As regards Iceland and Norway, this Framework Decision constitutes a development of provisions of the Schengen *acquis* within the meaning of the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the latter's association with the implementation, application and development of the Schengen *acquis* ([3]), which fall within the area referred to in Article 1, points H and I of Council Decision 1999/437/EC ([4]) on certain arrangements for the application of that Agreement.

(46) As regards Switzerland, this Framework Decision constitutes a development of the provisions of the Schengen *acquis* within the meaning of the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis* ([5]), which fall within the area referred to in Article 1, point H and I of Decision 1999/437/EC read in conjunction with Article 3 of Council Decision 2008/149/JHA ([6]) on the conclusion of that Agreement on behalf of the European Union.

(47) As regards Liechtenstein, this Framework Decision constitutes a development of the provisions of the Schengen *acquis* within the meaning of the Protocol signed between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis*, which fall within the area referred to in Article 1, point H and I of Decision 1999/437/EC read in conjunction with Article 3 of Council Decision 2008/262/JHA ([7]) on the signature of that Protocol on behalf of the European Union.

(48) This Framework Decision respects the fundamental rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union ([8]). This Framework Decision seeks to ensure full respect for the rights to privacy and the protection of personal data reflected in Articles 7 and 8 of the Charter,

HAS ADOPTED THIS FRAMEWORK DECISION:

Article 1

Purpose and scope

1. The purpose of this Framework Decision is to ensure a high level of protection of the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data in the framework of police and judicial cooperation in criminal matters, provided for by Title VI of the Treaty on European Union, while guaranteeing a high level of public safety.

2. In accordance with this Framework Decision, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy when, for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, personal data:

(a) are or have been transmitted or made available between Member States;

([1]) OJ L 131, 1.6.2000, p. 43.
([2]) OJ L 64, 7.3.2002, p. 20.
([3]) OJ L 176, 10.7.1999, p. 36.
([4]) OJ L 176, 10.7.1999, p. 31.
([5]) OJ L 53, 27.2.2008, p. 52.
([6]) OJ L 53, 27.2.2008, p. 50.
([7]) OJ L 83, 26.3.2008, p. 5.
([8]) OJ C 303, 14.12.2007, p. 1.

(b) are or have been transmitted or made available by Member States to authorities or to information systems established on the basis of Title VI of the Treaty on European Union; or

(c) are or have been transmitted or made available to the competent authorities of the Member States by authorities or information systems established on the basis of the Treaty on European Union or the Treaty establishing the European Community.

3. This Framework Decision shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means, of personal data which form part of a filing system or are intended to form part of a filing system.

4. This Framework Decision is without prejudice to essential national security interests and specific intelligence activities in the field of national security.

5. This Framework Decision shall not preclude Member States from providing, for the protection of personal data collected or processed at national level, higher safeguards than those established in this Framework Decision.

Article 2

Definitions

For the purposes of this Framework Decision:

(a) 'personal data' mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

(b) 'processing of personal data' and 'processing' mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

(c) 'blocking' means the marking of stored personal data with the aim of limiting their processing in future;

(d) 'personal data filing system' and 'filing system' mean any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

(e) 'processor' means any body which processes personal data on behalf of the controller;

(f) 'recipient' means any body to which data are disclosed;

(g) 'the data subject's consent' means any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed;

(h) 'competent authorities' mean agencies or bodies established by legal acts adopted by the Council pursuant to Title VI of the Treaty on European Union, as well as police, customs, judicial and other competent authorities of the Member States that are authorised by national law to process personal data within the scope of this Framework Decision;

(i) 'controller' means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data;

(j) 'referencing' means the marking of stored personal data without the aim of limiting their processing in future;

(k) 'to make anonymous' means to modify personal data in such a way that details of personal or material circumstances can no longer or only with disproportionate investment of time, cost and labour be attributed to an identified or identifiable natural person.

Article 3

Principles of lawfulness, proportionality and purpose

1. Personal data may be collected by the competent authorities only for specified, explicit and legitimate purposes in the framework of their tasks and may be processed only for the same purpose for which data were collected. Processing of the data shall be lawful and adequate, relevant and not excessive in relation to the purposes for which they are collected.

2. Further processing for another purpose shall be permitted in so far as:

(a) it is not incompatible with the purposes for which the data were collected;

(b) the competent authorities are authorised to process such data for such other purpose in accordance with the applicable legal provisions; and

(c) processing is necessary and proportionate to that other purpose.

The competent authorities may also further process the transmitted personal data for historical, statistical or scientific purposes, provided that Member States provide appropriate safeguards, such as making the data anonymous.

Article 4

Rectification, erasure and blocking

1. Personal data shall be rectified if inaccurate and, where this is possible and necessary, completed or updated.

2. Personal data shall be erased or made anonymous when they are no longer required for the purposes for which they were lawfully collected or are lawfully further processed. Archiving of those data in a separate data set for an appropriate period in accordance with national law shall not be affected by this provision.

3. Personal data shall be blocked instead of erased if there are reasonable grounds to believe that erasure could affect the legitimate interests of the data subject. Blocked data shall be processed only for the purpose which prevented their erasure.

4. When the personal data are contained in a judicial decision or record related to the issuance of a judicial decision, the rectification, erasure or blocking shall be carried out in accordance with national rules on judicial proceedings.

Article 5

Establishment of time limits for erasure and review

Appropriate time limits shall be established for the erasure of personal data or for a periodic review of the need for the storage of the data. Procedural measures shall ensure that these time limits are observed.

Article 6

Processing of special categories of data

The processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade-union membership and the processing of data concerning health or sex life shall be permitted only when this is strictly necessary and when the national law provides adequate safeguards.

Article 7

Automated individual decisions

A decision which produces an adverse legal effect for the data subject or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to the data subject shall be permitted only if authorised by a law which also lays down measures to safeguard the data subject's legitimate interests.

Article 8

Verification of quality of data that are transmitted or made available

1. The competent authorities shall take all reasonable steps to provide that personal data which are inaccurate, incomplete or no longer up to date are not transmitted or made available. To that end, the competent authorities shall, as far as practicable, verify the quality of personal data before they are transmitted or made available. As far as possible, in all transmissions of data, available information shall be added which enables the receiving Member State to assess the degree of accuracy, completeness, up-to-dateness and reliability. If personal data were transmitted without request the receiving authority shall verify without delay whether these data are necessary for the purpose for which they were transmitted.

2. If it emerges that incorrect data have been transmitted or data have been unlawfully transmitted, the recipient must be notified without delay. The data must be rectified, erased, or blocked without delay in accordance with Article 4.

Article 9

Time limits

1. Upon transmission or making available of the data, the transmitting authority may in line with the national law and in accordance with Articles 4 and 5, indicate the time limits for the retention of data, upon the expiry of which the recipient must erase or block the data or review whether or not they are still needed. This obligation shall not apply if, at the time of the expiry of these time limits, the data are required for a current investigation, prosecution of criminal offences or enforcement of criminal penalties.

2. Where the transmitting authority has not indicated a time limit in accordance with paragraph 1, the time limits referred to in Articles 4 and 5 for the retention of data provided for under the national law of the receiving Member State shall apply.

Article 10

Logging and documentation

1. All transmissions of personal data are to be logged or documented for the purposes of verification of the lawfulness of the data processing, self-monitoring and ensuring proper data integrity and security.

2. Logs or documentation prepared under paragraph 1 shall be communicated on request to the competent supervisory authority for the control of data protection. The competent supervisory authority shall use this information only for the control of data protection and for ensuring proper data processing as well as data integrity and security.

Article 11

Processing of personal data received from or made available by another Member State

Personal data received from or made available by the competent authority of another Member State may, in accordance with the requirements of Article 3(2), be further processed only for the following purposes other than those for which they were transmitted or made available:

(a) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties other than those for which they were transmitted or made available;

(b) other judicial and administrative proceedings directly related to the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties;

(c) the prevention of an immediate and serious threat to public security; or

(d) any other purpose only with the prior consent of the transmitting Member State or with the consent of the data subject, given in accordance with national law.

The competent authorities may also further process the transmitted personal data for historical, statistical or scientific purposes, provided that Member States provide appropriate safeguards, such as, for example, making the data anonymous.

Article 12

Compliance with national processing restrictions

1. Where, under the law of the transmitting Member State, specific processing restrictions apply in specific circumstances to data exchanges between competent authorities within that Member State, the transmitting authority shall inform the recipient of such restrictions. The recipient shall ensure that these processing restrictions are met.

2. When applying paragraph 1, Member States shall not apply restrictions regarding data transmissions to other Member States or to agencies or bodies established pursuant to Title VI of the Treaty on European Union other than those applicable to similar national data transmissions.

Article 13

Transfer to competent authorities in third States or to international bodies

1. Member States shall provide that personal data transmitted or made available by the competent authority of another Member State may be transferred to third States or international bodies, only if:

(a) it is necessary for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties;

(b) the receiving authority in the third State or receiving international body is responsible for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties;

(c) the Member State from which the data were obtained has given its consent to transfer in compliance with its national law; and

(d) the third State or international body concerned ensures an adequate level of protection for the intended data processing.

2. Transfer without prior consent in accordance with paragraph 1(c) shall be permitted only if transfer of the data is essential for the prevention of an immediate and serious threat to public security of a Member State or a third State or to essential interests of a Member State and the prior consent cannot be obtained in good time. The authority responsible for giving consent shall be informed without delay.

3. By way of derogation from paragraph 1(d), personal data may be transferred if:

(a) the national law of the Member State transferring the data so provides because of:

(i) legitimate specific interests of the data subject; or

(ii) legitimate prevailing interests, especially important public interests; or

(b) the third State or receiving international body provides safeguards which are deemed adequate by the Member State concerned according to its national law.

4. The adequacy of the level of protection referred to in paragraph 1(d) shall be assessed in the light of all the circumstances surrounding a data transfer operation or a set of data transfer operations. Particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the State of origin and the State or international body of final destination of the data, the rules of law, both general and sectoral, in force in the third State or international body in question and the professional rules and security measures which apply.

Article 14

Transmission to private parties in Member States

1. Member States shall provide that personal data received from or made available by the competent authority of another Member State may be transmitted to private parties only if:

(a) the competent authority of the Member State from which the data were obtained has consented to transmission in compliance with its national law;

(b) no legitimate specific interests of the data subject prevent transmission; and

(c) in particular cases transfer is essential for the competent authority transmitting the data to a private party for:

(i) the performance of a task lawfully assigned to it;

(ii) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties;

(iii) the prevention of an immediate and serious threat to public security; or

(iv) the prevention of serious harm to the rights of individuals.

2. The competent authority transmitting the data to a private party shall inform the latter of the purposes for which the data may exclusively be used.

Article 15

Information on request of the competent authority

The recipient shall, on request, inform the competent authority which transmitted or made available the personal data about their processing.

Article 16

Information for the data subject

1. Member States shall ensure that the data subject is informed regarding the collection or processing of personal data by their competent authorities, in accordance with national law.

2. When personal data have been transmitted or made available between Member States, each Member State may, in accordance with the provisions of its national law referred to in paragraph 1, ask that the other Member State does not inform the data subject. In such case the latter Member State shall not inform the data subject without the prior consent of the other Member State.

Article 17

Right of access

1. Every data subject shall have the right to obtain, following requests made at reasonable intervals, without constraint and without excessive delay or expense:

(a) at least a confirmation from the controller or from the national supervisory authority as to whether or not data relating to him have been transmitted or made available and information on the recipients or categories of recipients to whom the data have been disclosed and communication of the data undergoing processing; or

(b) at least a confirmation from the national supervisory authority that all necessary verifications have taken place.

2. The Member States may adopt legislative measures restricting access to information pursuant to paragraph 1(a), where such a restriction, with due regard for the legitimate interests of the person concerned, constitutes a necessary and proportional measure:

(a) to avoid obstructing official or legal inquiries, investigations or procedures;

(b) to avoid prejudicing the prevention, detection, investigation and prosecution of criminal offences or for the execution of criminal penalties;

(c) to protect public security;

(d) to protect national security;

(e) to protect the data subject or the rights and freedoms of others.

3. Any refusal or restriction of access shall be set out in writing to the data subject. At the same time, the factual or legal reasons on which the decision is based shall also be communicated to him. The latter communication may be omitted where a reason under paragraph 2(a) to (e) exists. In all of these cases the data subject shall be advised that he may appeal to the competent national supervisory authority, a judicial authority or to a court.

Article 18

Right to rectification, erasure or blocking

1. The data subject shall have the right to expect the controller to fulfil its duties in accordance with Articles 4, 8 and 9 concerning the rectification, erasure or blocking of personal data which arise from this Framework Decision. Member States shall lay down whether the data subject may assert this right directly against the controller or through the intermediary of the competent national supervisory authority. If the controller refuses rectification, erasure or blocking, the refusal must be communicated in writing to the data subject who must be informed of the possibilities provided for in national law for lodging a complaint or seeking judicial remedy. Upon examination of the complaint or judicial remedy, the data subject shall be informed whether the controller acted properly or not. Member States may also provide that the data subject shall be informed by the competent national supervisory authority that a review has taken place.

2. If the accuracy of an item of personal data is contested by the data subject and its accuracy or inaccuracy cannot be ascertained, referencing of that item of data may take place.

Article 19

Right to compensation

1. Any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Framework Decision shall be entitled to receive compensation for the damage suffered from the controller or other authority competent under national law.

2. Where a competent authority of a Member State has transmitted personal data, the recipient cannot, in the context of its liability vis-à-vis the injured party in accordance with national law, cite in its defence that the data transmitted were inaccurate. If the recipient pays compensation for damage caused by the use of incorrectly transmitted data, the transmitting competent authority shall refund to the recipient the amount paid in damages, taking into account any fault that may lie with the recipient.

Article 20

Judicial remedies

Without prejudice to any administrative remedy for which provision may be made prior to referral to the judicial authority, the data subject shall have the right to a judicial remedy for any breach of the rights guaranteed to him by the applicable national law.

Article 21

Confidentiality of processing

1. Any person who has access to personal data which fall within the scope of this Framework Decision may process such data only if that person is a member of, or acts on instructions of, the competent authority, unless he is required to do so by law.

2. Persons working for a competent authority of a Member State shall be bound by all the data protection rules which apply to the competent authority in question.

Article 22

Security of processing

1. Member States shall provide that the competent authorities must implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission over a network or the making available by granting direct automated access, and against all other unlawful forms of processing, taking into account in particular the risks represented by the processing and the nature of the data to be protected. Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

2. In respect of automated data processing each Member State shall implement measures designed to:

(a) deny unauthorised persons access to data-processing equipment used for processing personal data (equipment access control);

(b) prevent the unauthorised reading, copying, modification or removal of data media (data media control);

(c) prevent the unauthorised input of data and the unauthorised inspection, modification or deletion of stored personal data (storage control);

(d) prevent the use of automated data-processing systems by unauthorised persons using data communication equipment (user control);

(e) ensure that persons authorised to use an automated data-processing system only have access to the data covered by their access authorisation (data access control);

(f) ensure that it is possible to verify and establish to which bodies personal data have been or may be transmitted or made available using data communication equipment (communication control);

(g) ensure that it is subsequently possible to verify and establish which personal data have been input into automated data-processing systems and when and by whom the data were input (input control);

(h) prevent the unauthorised reading, copying, modification or deletion of personal data during transfers of personal data or during transportation of data media (transport control);

(i) ensure that installed systems may, in case of interruption, be restored (recovery);

(j) ensure that the functions of the system perform, that the appearance of faults in the functions is reported (reliability) and that stored data cannot be corrupted by means of a malfunctioning of the system (integrity).

3. Member States shall provide that processors may be designated only if they guarantee that they observe the requisite technical and organisational measures under paragraph 1 and comply with the instructions under Article 21. The competent authority shall monitor the processor in those respects.

4. Personal data may be processed by a processor only on the basis of a legal act or a written contract.

Article 23

Prior consultation

Member States shall ensure that the competent national supervisory authorities are consulted prior to the processing of personal data which will form part of a new filing system to be created where:

(a) special categories of data referred to in Article 6 are to be processed; or

(b) the type of processing, in particular using new technologies, mechanism or procedures, holds otherwise specific risks for the fundamental rights and freedoms, and in particular the privacy, of the data subject.

Article 24

Penalties

Member States shall adopt suitable measures to ensure the full implementation of the provisions of this Framework Decision and shall in particular lay down effective, proportionate and dissuasive penalties to be imposed in case of infringements of the provisions adopted pursuant to this Framework Decision.

Article 25

National supervisory authorities

1. Each Member State shall provide that one or more public authorities are responsible for advising and monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Framework Decision. These authorities shall act with complete independence in exercising the functions entrusted to them.

2. Each authority shall in particular be endowed with:

(a) investigative powers, such as powers of access to data forming the subject matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties;

(b) effective powers of intervention, such as, for example, that of delivering opinions before processing operations are carried out, and ensuring appropriate publication of such opinions, of ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing, of warning or admonishing the controller, or that of referring the matter to national parliaments or other political institutions;

(c) the power to engage in legal proceedings where the national provisions adopted pursuant to this Framework Decision have been infringed or to bring this infringement to the attention of the judicial authorities. Decisions by the supervisory authority which give rise to complaints may be appealed against through the courts.

3. Each supervisory authority shall hear claims lodged by any person concerning the protection of his rights and freedoms in regard to the processing of personal data. The person concerned shall be informed of the outcome of the claim.

4. Member States shall provide that the members and staff of the supervisory authority are bound by the data protection provisions applicable to the competent authority in question and, even after their employment has ended, are to be subject to a duty of professional secrecy with regard to confidential information to which they have access.

Article 26

Relationship to agreements with third States

This Framework Decision is without prejudice to any obligations and commitments incumbent upon Member States or upon the Union by virtue of bilateral and/or multilateral agreements with third States existing at the time of adoption of this Framework Decision.

In the application of these agreements, the transfer to a third State of personal data obtained from another Member State, shall be carried out while respecting Article 13(1)(c) or (2), as appropriate.

Article 27

Evaluation

1. Member States shall report to the Commission by 27 November 2013 on the national measures they have taken to ensure full compliance with this Framework Decision, and particularly with regard to those provisions that already have to be complied with when data is collected. The Commission shall examine in particular the implications of those provisions for the scope of this Framework Decision as laid down in Article 1(2).

2. The Commission shall report to the European Parliament and the Council within one year on the outcome of the evaluation referred to in paragraph 1, and shall accompany its report with any appropriate proposals for amendments to this Framework Decision.

Article 28

Relationship to previously adopted acts of the Union

Where in acts, adopted under Title VI of the Treaty on European Union prior to the date of entry into force of this Framework Decision and regulating the exchange of personal data between Member States or the access of designated authorities of Member States to information systems established pursuant to the Treaty establishing the European Community, specific conditions have been introduced as to the use of such data by the receiving Member State, these conditions shall take precedence over the provisions of this Framework Decision on the use of data received from or made available by another Member State.

Article 29

Implementation

1. Member States shall take the necessary measures to comply with the provisions of this Framework Decision before 27 November 2010.

2. By the same date Member States shall transmit to the General Secretariat of the Council and to the Commission the text of the provisions transposing into their national law the obligations imposed on them under this Framework Decision, as well as information on the supervisory authorities referred to in Article 25. On the basis of a report established using this information by the Commission, the Council shall, before 27 November 2011, assess the extent to which Member States have complied with the provisions of this Framework Decision.

Article 30

Entry into force

This Framework Decision shall enter into force on the 20th day following its publication in the *Official Journal of the European Union*.

Done at Brussels, 27 November 2008.

For the Council

The President

M. ALLIOT-MARIE

10/31/2010

Appendix Seven

Data Protection Vision 2020

options for improving European policy and legislation during 2010-2020

Joseph A. Cannataci

Lege nr. 238 din 10/06/2009

Publicat in Monitorul Oficial, Partea I nr. 405 din 15/06/2009
Intrare in vigoare: 18/06/2009

privind reglementarea prelucrării datelor cu caracter personal de către structurile/unităţile Ministerului Administraţiei şi Internelor în activităţile de prevenire, cercetare şi combatere a infracţiunilor, precum şi de menţinere şi asigurare a ordinii publice

Publicat în 15/06/2009

Afişează fişa actului

Acţiune	Act	Data acţiune	Titlu act
Promulgat prin	Decret nr. 936 din 09/06/2009	15/06/2009	pentru promulgarea Legii privind reglementarea prelucrării datelor cu caracter personal de către str...

Parlamentul României adoptă prezenta lege.

CAPITOLUL I
Dispoziţii generale

Art. 1. - (1) Prezenta lege reglementează prelucrarea automată şi neautomată a datelor cu caracter personal pentru realizarea activităţilor de prevenire, cercetare şi combatere a infracţiunilor, cât şi de menţinere şi asigurare a ordinii publice de către structurile/unităţile Ministerului Administraţiei şi Internelor, potrivit competenţelor acestora.
(2) Structurile/unităţile Ministerului Administraţiei şi Internelor, denumite în continuare structurile/unităţile M.A.I., care desfăşoară, potrivit competenţelor, activităţile prevăzute la alin. (1), în calitate de operatori, dobândite în condiţiile Legii nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date, cu modificările şi completările ulterioare, prelucrează date cu caracter personal în exercitarea atribuţiilor legale.
Art. 2. - (1) Pentru realizarea activităţilor prevăzute la art. 1 alin. (1), structurile/unităţile M.A.I. constituie, organizează şi deţin, potrivit atribuţiilor legale, sisteme de evidenţă şi utilizează mijloace automate şi neautomate de prelucrare a datelor cu caracter personal, în condiţiile legii.
(2) Structurile/unităţile M.A.I. utilizează sisteme de evidenţă şi/sau mijloace automate şi neautomate de prelucrare a datelor cu caracter personal, cu respectarea drepturilor omului şi aplicarea principiilor legalităţii, necesităţii, confidenţialităţii, proporţionalităţii şi numai dacă, prin utilizarea acestora, este asigurată protecţia datelor prelucrate.
(3) Înaintea introducerii unui sistem de evidenţă sau a unui mijloc automat/neautomat de prelucrare a datelor cu caracter personal care este susceptibil să prezinte anumite riscuri privind datele prelucrate, structurile/unităţile M.A.I. consultă Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal, denumită în continuare Autoritatea naţională de supraveghere, care, dacă este cazul, stabileşte garanţii adecvate, potrivit legii.

CAPITOLUL II
Notificarea prelucrărilor datelor cu caracter personal

Art. 3. - (1) Prelucrările de date cu caracter personal sunt notificate Autorităţii naţionale de supraveghere. Notificarea se efectuează anterior oricărei prelucrări, în condiţiile legii.
(2) Notificarea prelucrării automate sau neautomate a datelor cu caracter personal prin sisteme de evidenţă a datelor cu caracter personal, realizată potrivit legii de către structurile/unităţile M.A.I., cuprinde, pe lângă informaţiile prevăzute la art. 22 alin. (8) din Legea nr. 677/2001, cu modificările şi completările ulterioare, în mod corespunzător şi informaţii referitoare la natura fiecărui sistem de evidenţă a datelor cu caracter personal care are legătură cu prelucrarea, precum şi la destinatarii cărora le sunt comunicate datele.

(3) Notificarea prelucrării datelor cu caracter personal prin sisteme de evidenţă constituite în anumite cazuri numai pentru perioada necesară realizării unor activităţi de prevenire, cercetare şi combatere a infracţiunilor, precum şi de menţinere şi asigurare a ordinii publice se face cu respectarea condiţiilor prevăzute la alin. (2), numai dacă prelucrarea nu a făcut obiectul unei notificări anterioare.

CAPITOLUL III
Colectarea datelor cu caracter personal

Art. 4. - (1) Pentru realizarea activităţilor prevăzute la art. 1 alin. (1), structurile/unităţile M.A.I. colectează date cu caracter personal, cu sau fără consimţământul persoanei vizate, în condiţiile legii.
(2) Colectarea datelor cu caracter personal fără consimţământul persoanei vizate pentru realizarea activităţilor prevăzute la art. 1 alin. (1) se face numai dacă această măsură este necesară pentru prevenirea unui pericol iminent cel puţin asupra vieţii, integrităţii corporale sau sănătăţii unei persoane ori a proprietăţii acesteia, precum şi pentru combaterea unei anumite infracţiuni.
(3) Colectarea datelor cu caracter personal pentru realizarea activităţilor prevăzute la art. 1 alin. (1) se efectuează de personalul structurilor/unităţilor M.A.I. numai în scopul îndeplinirii atribuţiilor de serviciu.
(4) Colectarea datelor cu caracter personal în scopurile prevăzute la art. 1 alin. (1) trebuie să fie limitată la datele necesare pentru prevenirea unui pericol iminent cel puţin asupra vieţii, integrităţii corporale sau sănătăţii unei persoane ori a proprietăţii acesteia, precum şi pentru combaterea unei anumite infracţiuni.
(5) Colectarea de date privind persoana fizică exclusiv datorită faptului că aceasta are o anumită origine rasială, anumite convingeri religioase ori politice, un anumit comportament sexual sau datorită apartenenţei acesteia la anumite mişcări ori organizaţii care nu contravin legii este interzisă.
(6) Prin excepţie de la prevederile alin. (5), structurile/unităţile M.A.I. colectează şi prelucrează, cu respectarea garanţiilor prevăzute de Legea nr. 677/2001, cu modificările şi completările ulterioare, date exclusiv în baza acestor criterii numai dacă, într-un caz determinat, sunt necesare pentru efectuarea actelor premergătoare sau a urmăririi penale, ca urmare a săvârşirii unei infracţiuni. Prevederile art. 3 se aplică în mod corespunzător.
(7) Prevederile alin. (6) nu aduc atingere dispoziţiilor legale care reglementează obligaţia autorităţilor publice de a respecta şi de a ocroti viaţa intimă, familială şi privată.

CAPITOLUL IV
Stocarea datelor cu caracter personal

Art. 5. - (1) Pentru realizarea scopurilor activităţilor prevăzute la art. 1 alin. (1), structurile/unităţile M.A.I. stochează numai acele date cu caracter personal care sunt exacte, complete şi necesare îndeplinirii atribuţiilor legale sau obligaţiilor rezultate din instrumente juridice internaţionale la care România este parte.
(2) Stocarea diferitelor categorii de date cu caracter personal se realizează prin ordonarea acestora în funcţie de gradul lor de acurateţe şi exactitate. Datele cu caracter personal bazate pe opinii şi interpretări personale rezultate din activităţile prevăzute la art. 1 alin. (1) sunt ordonate în mod distinct.
(3) Structurile/unităţile M.A.I. au obligaţia de a verifica periodic calitatea datelor prevăzute la alin. (2), conform regulilor stabilite potrivit art. 14 alin. (1) lit. b).
(4) În situaţia în care datele cu caracter personal stocate se dovedesc a fi inexacte sau incomplete, structurile/unităţile M.A.I. care le deţin au obligaţia să le şteargă, distrugă, modifice, actualizeze sau, după caz, să le completeze.
(5) Structurile/unităţile M.A.I. stochează datele cu caracter personal colectate în scopuri administrative separat de datele cu caracter personal colectate în scopurile prevăzute la art. 1 alin. (1).

CAPITOLUL V
Comunicarea datelor cu caracter personal

Art. 6. - (1) Comunicarea datelor cu caracter personal între structurile/unităţile M.A.I. se face numai în cazul în care este necesară pentru exercitarea competenţelor şi îndeplinirea atribuţiilor legale ce le revin.
(2) Comunicarea de date cu caracter personal către alte autorităţi sau instituţii publice se poate efectua numai în următoarele situaţii:
a) în baza unei prevederi legale exprese ori cu autorizarea Autorităţii naţionale de supraveghere;

b) când datele sunt indispensabile îndeplinirii atribuţiilor legale ale destinatarului şi numai dacă scopul în care se face colectarea sau prelucrarea de către destinatar nu este incompatibil cu scopul pentru care datele au fost colectate de structurile/unităţile M.A.I., iar comunicarea datelor de structurile/unităţile M.A.I. se realizează în conformitate cu atribuţiile legale ale acestora.

(3) Prin excepţie de la prevederile alin. (2), comunicarea datelor cu caracter personal către alte autorităţi sau instituţii publice este permisă în următoarele situaţii:

a) persoana vizată şi-a exprimat consimţământul expres şi neechivoc pentru comunicarea datelor sale;

b) comunicarea este necesară pentru a preveni un pericol grav şi iminent cel puţin asupra vieţii, integrităţii corporale sau sănătăţii unei persoane ori a proprietăţii acesteia.

(4) Comunicarea datelor cu caracter personal către entităţi de drept privat care îşi desfăşoară activitatea pe teritoriul României se efectuează numai dacă există o obligaţie legală expresă sau cu autorizarea Autorităţii naţionale de supraveghere.

(5) Prin excepţie de la prevederile alin. (4), comunicarea datelor cu caracter personal către entităţi de drept privat care îşi desfăşoară activitatea pe teritoriul României sau în afara acestuia este permisă dacă persoana vizată şi-a dat consimţământul în mod expres şi neechivoc pentru comunicarea datelor sale sau dacă este necesară pentru a preveni un pericol grav şi iminent cel puţin asupra vieţii, integrităţii corporale sau sănătăţii unei persoane ori a proprietăţii acesteia sau a unei alte persoane ameninţate.

Art. 7. - Datele cu caracter personal deţinute de structurile/unităţile M.A.I. potrivit scopurilor prevăzute la art. 1 alin. (1) pot fi transferate către Organizaţia Internaţională a Poliţiei Criminale - Interpol, Oficiul European de Poliţie - Europol sau alte instituţii internaţionale similare, precum şi către organismele de poliţie ale altor state, dacă există o prevedere legală expresă în legislaţia naţională sau într-un acord internaţional ratificat de România ori prevederi care reglementează cooperarea judiciară internaţională în materie penală sau, în lipsa unei astfel de prevederi, când transferul este necesar pentru prevenirea unui pericol grav şi iminent asupra vieţii, integrităţii corporale sau sănătăţii unei persoane ori a proprietăţii acesteia, precum şi pentru combaterea unei infracţiuni grave prevăzute de lege, cu respectarea legii române.

Art. 8. - (1) Cererile pentru comunicarea datelor cu caracter personal adresate structurilor/unităţilor M.A.I. de către alte structuri/unităţi ale M.A.I., alte autorităţi sau instituţii publice, entităţi de drept privat care îşi desfăşoară activitatea pe teritoriul României sau în afara acestuia şi organisme de poliţie ale altor state trebuie să conţină datele de identificare a solicitantului, precum şi motivarea şi scopul cererii, conform prevederilor legale interne sau celor cuprinse în acordurile internaţionale la care România este parte. Cererile care nu conţin aceste date şi nu sunt conforme prevederilor legale interne sau celor cuprinse în acordurile internaţionale la care România este parte se resping.

(2) Înainte de comunicare, structurile/unităţile M.A.I. verifică dacă datele solicitate sunt exacte, complete şi actualizate. În cazul în care se constată că nu sunt corecte, complete sau actualizate, datele nu se comunică. În comunicări trebuie indicate, după caz, datele care rezultă din hotărâri ale instanţelor judecătoreşti ori din actele prin care s-a dispus neînceperea urmăririi penale, clasarea, scoaterea de sub urmărire penală, încetarea urmăririi penale sau trimiterea în judecată, precum şi datele bazate pe opinii şi interpretări personale rezultate din activităţile prevăzute la art. 1 alin. (1). Datele bazate pe opinii şi interpretări personale rezultate din activităţile prevăzute la art. 1 alin. (1) trebuie verificate la sursă înainte de a fi comunicate, iar gradul de acurateţe şi exactitate al acestor date trebuie întotdeauna menţionat cu ocazia comunicării.

(3) În situaţia în care au fost transmise date incorecte sau neactualizate, structurile/unităţile M.A.I. au obligaţia să îi informeze pe destinatarii respectivelor date asupra neconformităţii acestora, cu menţionarea datelor care au fost modificate.

Art. 9. - (1) La comunicarea datelor cu caracter personal către alte autorităţi sau instituţii publice, entităţi de drept privat care îşi desfăşoară activitatea pe teritoriul României sau în afara acestuia, Organizaţia Internaţională a Poliţiei Criminale - Interpol, Oficiul European de Poliţie - Europol sau alte instituţii internaţionale similare ori către organisme de poliţie ale altor state, structurile/unităţile M.A.I. atenţionează destinatarii asupra interdicţiei de a prelucra datele comunicate în alte scopuri decât cele specificate în cererea de comunicare.

(2) Prelucrarea datelor de către destinatari în alte scopuri decât cele care au format obiectul cererii se poate realiza numai cu acordul structurilor/unităţilor M.A.I. care le-au comunicat şi numai cu respectarea prevederilor art. 6 alin. (2)-(5) şi ale art. 7.

Art. 10. - (1) Pentru realizarea activităţilor de cercetare şi combatere a infracţiunilor, structurile/unităţile M.A.I. pot interconecta sistemele de evidenţă a datelor cu caracter personal sau, după caz, mijloacele automate de prelucrare a datelor cu caracter personal pe care le deţin pentru scopuri diferite.

(2) În scopul prevăzut la alin. (1), interconectarea se poate realiza şi cu sistemele de evidenţă sau cu mijloacele automate de prelucrare a datelor cu caracter personal deţinute de alţi operatori.

(3) Interconectările prevăzute la alin. (1) şi (2) sunt permise numai în cazul efectuării actelor premergătoare, al urmăririi penale sau al judecării unei infracţiuni în baza unei autorizări emise de procurorul competent să efectueze sau să supravegheze, într-un caz determinat, efectuarea actelor premergătoare sau

urmărirea penală ori, în cazul judecării unei infracţiuni, de judecătorul anume desemnat de la instanţa căreia îi revine competenţa de a judeca fondul cauzei pentru care sunt prelucrate datele respective.

(4) Accesul direct sau printr-un serviciu de comunicaţii electronice la un sistem de evidenţă a datelor cu caracter personal care face obiectul interconectării, potrivit alin. (1), este permis numai în condiţiile legii şi cu respectarea prevederilor art. 1 alin. (1) şi ale art. 5-11.

(5) Interconectarea sistemelor de evidenţă a datelor cu caracter personal sau a mijloacelor automate de prelucrare a datelor cu caracter personal nu se realizează în cazul activităţilor de prevenire a infracţiunilor, de menţinere şi de asigurare a ordinii publice.

CAPITOLUL VI
Drepturile persoanei vizate

Art. 11. - **(1)** Structurile/unităţile M.A.I. asigură condiţiile de exercitare a drepturilor conferite de lege persoanei vizate, cu respectarea Legii nr. 677/2001, cu modificările şi completările ulterioare, şi a prezentei legi.

(2) Prevederile referitoare la exercitarea drepturilor persoanei vizate, prevăzute de Legea nr. 677/2001, cu modificările şi completările ulterioare, nu se aplică pe perioada în care o asemenea măsură este necesară pentru evitarea prejudicierii activităţilor specifice de prevenire, cercetare şi combatere a infracţiunilor, precum şi de menţinere şi asigurare a ordinii publice, ca urmare a cunoaşterii de persoana vizată a faptului că datele sale cu caracter personal sunt prelucrate, sau este necesară pentru protejarea persoanei vizate ori a drepturilor şi libertăţilor altor persoane, în cazul în care există date şi informaţii că aceste drepturi şi libertăţi sunt puse în pericol.

(3) În cazul aplicării excepţiilor de la exercitarea drepturilor persoanei vizate, prevăzute la alin. (2), acestea trebuie motivate în scris. Necomunicarea motivelor este posibilă numai în măsura în care este necesară bunei desfăşurări a activităţilor prevăzute la art. 1 alin. (1) sau pentru protejarea drepturilor şi libertăţilor altor persoane decât persoana vizată.

(4) În toate situaţiile, persoana vizată va fi informată cu privire la dreptul de a se adresa Autorităţii naţionale de supraveghere sau, după caz, instanţei de judecată, care va decide dacă măsurile luate de structurile/unităţile M.A.I., conform prevederilor alin. (2), sunt întemeiate.

(5) În situaţia în care, în urma exercitării dreptului de acces sau a dreptului de intervenţie, rezultă că datele cu caracter personal sunt inexacte, irelevante sau înregistrate în mod abuziv, acestea vor fi şterse sau rectificate prin anexarea unui document, încheiat în acest sens, la sistemul de evidenţă ale cărui date cu caracter personal au suferit modificări, deţinut de structurile/unităţile M.A.I.

(6) Măsurile prevăzute la alin. (5) se aplică tuturor documentelor care au legătură cu sistemul de evidenţă a datelor cu caracter personal. În cazul în care acestea nu sunt efectuate imediat, se va avea în vedere realizarea lor cel mai târziu la data prelucrării ulterioare a datelor cu caracter personal sau la o următoare comunicare a acestora.

CAPITOLUL VII
Încheierea operaţiunilor de prelucrare a datelor cu caracter personal

Art. 12. - **(1)** Datele cu caracter personal stocate în îndeplinirea activităţilor prevăzute la art. 1 alin. (1) se şterg atunci când nu mai sunt necesare scopurilor pentru care au fost colectate.

(2) Înainte de ştergerea datelor cu caracter personal, potrivit alin. (1), şi dacă activităţile prevăzute la art. 1 alin. (1) nu mai pot fi prejudiciate prin cunoaşterea faptului că datele cu caracter personal au fost colectate şi stocate, persoana vizată trebuie informată atunci când colectarea şi stocarea datelor s-au efectuat fără consimţământul său.

(3) În condiţiile prevăzute la alin. (2), informarea persoanei vizate se realizează de structurile/unităţile M.A.I. care au colectat şi stocat datele cu caracter personal ale acesteia, în termen de 15 zile de la momentul în care activităţile prevăzute la art. 1 alin. (1) nu mai pot fi prejudiciate sau, după caz, de la momentul comunicării către aceste structuri/unităţi ale M.A.I. a unei soluţii de neîncepere a urmăririi penale, clasare, scoatere de sub urmărire penală sau încetare a urmăririi penale.

(4) Prin excepţie de la prevederile alin. (1), datele cu caracter personal pot fi stocate şi după îndeplinirea scopurilor pentru care au fost colectate, dacă este necesară păstrarea acestora. Evaluarea necesităţii stocării datelor după îndeplinirea scopurilor pentru care au fost colectate se realizează, în special, în următoarele situaţii:

a) datele sunt necesare în vederea terminării urmăririi penale într-un caz determinat;

b) nu există o hotărâre judecătorească definitivă;
c) nu a intervenit reabilitarea;
d) nu a intervenit prescripţia executării pedepsei;
e) nu a intervenit amnistia;
f) datele fac parte din categorii speciale de date, potrivit Legii nr. 677/2001, cu modificările şi completările ulterioare.

CAPITOLUL VIII
Securitatea datelor cu caracter personal

Art. 13. - Structurile/unităţile M.A.I. sunt obligate să ia toate măsurile necesare pentru a asigura securitatea tehnică şi organizatorică adecvată a prelucrării datelor cu caracter personal, astfel încât să prevină accesul, comunicarea sau distrugerea neautorizată ori alterarea datelor. În acest scop, se au în vedere diferitele caracteristici ale sistemelor de evidenţă a datelor cu caracter personal şi conţinutul acestora.

CAPITOLUL IX
Dispoziţii finale

Art. 14. - **(1)** Structurile/unităţile M.A.I. care desfăşoară activităţile prevăzute la art. 1 alin. (1) au obligaţia de a elabora reguli, dacă acestea nu sunt stabilite prin prevederi legale exprese, cu privire la:
a) termenele de stocare a datelor cu caracter personal pe care le prelucrează;
b) verificările periodice asupra datelor cu caracter personal pentru ca acestea să fie exacte, actuale şi complete;
c) ştergerea datelor cu caracter personal.
(2) În lipsa unor prevederi legale exprese care să stabilească regulile prevăzute la alin. (1), structurile/unităţile M.A.I. care desfăşoară activităţile prevăzute la art. 1 alin. (1) au obligaţia ca, în termen de 30 de zile de la data intrării în vigoare a prezentei legi, să stabilească aceste reguli, cu avizul Autorităţii naţionale de supraveghere acordat în condiţiile legii.
Art. 15. - Prevederile prezentei legi se completează cu dispoziţiile Legii nr. 677/2001, cu modificările şi completările ulterioare.

Această lege a fost adoptată de Parlamentul României, cu respectarea prevederilor art. 75 şi ale art. 76 alin. (2) din Constituţia României, republicată.

Bucureşti, 10 iunie 2009.
Nr. 238.

10/31/2010

Appendix Eight

Data Protection Vision 2020

options for improving European policy and legislation during 2010-2020

Joseph A. Cannataci