WORKING
PAPER

Review of EU Data Protection Directive

Inception Report

NEIL ROBINSON, HANS GRAUX AND
MAARTEN BOTTERMAN

WR-607-ICO

August 2008

Prepared for the Information Commissioner's Office by RAND Europe, time.lex and GNKS-Consult

EUROPE

Preface

RAND Europe, time.lex and GNKS-Consult have joined together in a project team led by RAND Europe to meet the requirements of the UK Information Commissioner's Office for a review of the EU Data Protection Directive 95/46/EC. A literature review, key informant interviews and a scenario based workshop will all be used to assess the strengths and weaknesses of the EU Data Protection Directive and identify promising avenues for improvements in its application.

Researchers from each organisation have considerable experience working together on studies in the fields of law, information technology and policy regarding security, identity and privacy aspects of Information Communications Technology. Recent studies conducted for DG Information Society and Media at the European Commission, most notably the currently ongoing study on a *Vision for eGovernment towards 2020*, the 2007 studies on a *Comparison of Privacy and Trust Policies* and on the *Impact of Security Aspects on the revision of the EU Communications Framework*; and others as well as *the work for IAAC on Identity Management and* the 2005 Scenario study for the Cyber Trust and Crime Prevention initiative for the UK Foresight Office illustrate the track record of relevant projects conducted in this field.

This study comes at a time of heightened policy interest in personal data. Increasing public interest across Europe about data protection, combined with calls for reform of the Data Protection Directive from various stakeholders means that the conduct of this study will be closely observed. This is why it is important that an independent and objective view is taken of the strengths and weaknesses of the Directive and possible avenues for improvement.

This report, part of RAND's Working Paper series, represents the Inception Report (IR) for the study and as such should be read as the indicative starting point for the study. This report was jointly prepared by RAND Europe, time.lex and GNKS-Consult.

Information on each of the consortium members can be found on their respective web-pages:

RAND Europe	time.lex	GNKS-Consult
www.rand.org/randeurope	www.timelex.eu	www.gnksconsult.com

For more information about this study please email dataprotectionstudy@rand.org.

Contents

Summary

The UK Information Commissioner's Office (ICO) would like to commission a review into the EU Data Protection Directive 95/46/EC, specifically its strengths and weaknesses and potential avenues for improvement of its application. This review will address concerns that certain provisions of the Directive may no longer optimally serve their purpose of protecting data subjects against abuses of their personal data, especially given existing technical and societal changes that seem to increasingly favour facilitated and extended use of such data. The study will consider a number of issues arising from the application of the Directive and its impact by reviewing the broad canon of research available in this domain.

This Inception Report (IR) is an amended version of the original proposal submitted as a response to the tender from the ICO in April 2008 and describes in general terms our approach. It also details what we regard to be the drivers and current contextual situation with regard to the Data Protection Directive. Finally, descriptions of the team members and each organisation involved are provided to demonstrate our track record.

The issues analysis will be accomplished by desk research into the aspects of the Directive that are difficult to apply in practice or which do not contribute substantially to meeting its goals, supported by a focused set of interviews of key stakeholders to validate the information gathered. Exploration of promising avenues for the improvement of the regulatory landscape will be accomplished in a 'back-casting' style policy-orientated scenario workshop with a small number of carefully chosen participants.

The team has undertaken a range of policy research studies previously conducted in the domain of privacy, EU law, identity management, information assurance, self and co-regulation and regulatory evaluation. Team members have a longstanding robust working relationship. Researchers from each organisation have considerable experience working together on studies in the fields of law, information technology and policy regarding security, identity and privacy aspects of Information Communications Technology. Recent studies conducted for DG Information Society and Media at the European Commission, including the currently ongoing study on a *Vision for eGovernment towards 2020*, the 2007 studies on a *Comparison of Privacy and Trust Policies* and on the *Impact of Security Aspects on the revision of the EU Communications Framework*; a 2006 study into the *Security Challenges posed by Disruptive Technologies*, the 2005 *Legal Handbook of Computer and Network Misuse in EU Countries*; the *2006 MODINIS eIDM study* and the *IDABC eIDM interoperability initiatives, as well as the work for IAAC on Identity Management and* the 2005 Scenario study for the Cyber Trust and Crime Prevention initiative for the British Foresight Office illustrate the track record of relevant projects conducted in this field.

CHAPTER 1 Objectives and Tasks

1.1 Objective

The Information Commissioner's Office (ICO) has called for a review into the EU Data Protection Directive, given the pace of technological change, continuing pressure upon personal information and increasing awareness from the general public about the environment for the use of personal information and breaches.

This study will review the strengths and weaknesses of the EU Data Protection Directive 95/46/EC and its current application in practice, and identify promising avenues (both general and specific) for improving the Data Protection Directive towards the future, taking account the global context in which it impacts and the interests of a multitude of stakeholders.

1.2 Our Approach

To do this, the study will analyse existing empirical data on the Data Protection Directive and its application through desk research and interviews with key stakeholders. We will then use our appreciation of the social, technological and policy contexts to compare and refine the indicative list of questions and issues outlined in the Invitation to Tender. Our approach will build upon the existing body of knowledge and also take advantage of ongoing research activities (specifically, a RAND Europe conducted quantitative study of preferences to privacy, security and liberty and a set of scenarios developed over the course of previous work conducted by this team). These will be updated based on new understanding of the domain.

The literature study will be complemented with interviews with stakeholders and experts knowledgeable about the strengths and weaknesses of the Data Protection Directive. Interviewee candidates include the European Data Protection Supervisor, European Data Protection Authorities, similar regulatory bodies from other jurisdictions (e.g. Canada, Australia) data controllers from the public and private sector and civil society groups as well as researchers and academics. The interviews will be used to validate and balance the results from the literature review and help identify the main issues to be addressed regarding privacy and data protection towards the future.

Following the period of desk research and interviews, constituting the main phase of this work, the study will use a scenario-based workshop to identify, across the stakeholder groups of Citizens, Business and Administration represented at the workshop, what 'levers' need to be 'pulled' now to get to a world in the future where the Data Protection Directive is working in the best way possible.

It is assumed that the principles set out in the Directive are sound but rather the challenge will be to find ways to improve their achievement in practice, while identifying possible future developments and assessing how these may affect the relevance and impact of the Directive.

This review of the EU Data Protection Directive could also make a significant contribution to European debate into a possible consolidated and modernised data protection instrument applicable across both the Internal Market (so called 1st pillar) and police and judicial co-operation matters in the 3rd pillar. Furthermore, the remit of this review builds upon statements by the European Data Protection Supervisor (EDPS) in his Opinion of 27th November 2007 that amendment of the Directive is inevitable, yet not before full implementation in the Member States is witnessed.[1]

By commissioning such a review it is assumed that the ICO also hopes to build upon the impact of other similarly commissioned ICO studies, most notably the 2006 Report by the Surveillance Studies Group into the Surveillance Society, distributed at the 28th International Conference of Data Protection and Privacy Commissioners.[2]

1.3 Suitability of the Study Team

The study team of RAND Europe, time.lex and GNKS-Consult contains experts that cover a broad range of multidisciplinary skills and societal, legal, economic, technical and policy expertise. This makes the team uniquely qualified to provide high quality outputs to help the Information Commissioner achieve these aims. We will aim to deliver outputs that are practical, realistic and implementable from a policy perspective. In particular there are several reasons why our team specifically meets the requirement.

- The study team will approach the task with a view to bringing perspectives from different domains and which is not based on a formulaic legal assessment. The team has strong complementarity in domains such as policy research, legal analysis, economics, information technology and data protection knowledge.
- Although we can call upon specific legal knowledge in this area the study team will not confine themselves to a narrow legal understanding but rather will base their

[1] Hustinx, P., *Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council on the follow up of the Work Programme for better implementation of the Data Protection Directive* Opinions of the European Data Protection Supervisor Official Journal of the European Union C 255 27th October 2007 p 2

[2] Surveillance Studies Network; *A Report on the Surveillance Society* http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf Information Commissioner's Office; September 2006

analysis on what is practically implementable (taking into account the institutional landscape of EU legislation and the complexities of multi-pillar structure of the EU.

- Our team will provide a balanced, non-partisan, objective and independent analysis of these issues that is not pressing one particular viewpoint, but rather whose conclusions will be soundly based on evidence and research.
- Our team has been collaborating in important EU studies in this domain for the last 8 years.
- We will provide a view that is relevant to the UK given our understanding of the peculiarities of the national environment with consideration of the wider European and indeed global context.

CHAPTER 2 Background and Context

2.1 Introduction

In this chapter we present an overview of the background and historical context of the Data Protection Directive; why current factors, such as pressure on privacy, evolving information governance and technology need to be understood in order to appreciate why its effectiveness is being undermined; different ways in which personal data can be protected (such as legislation, self- and co-regulation and technology) and finally a brief understanding of issues that would need to be taken into context in any revision or amendment along with what this context means for our study.

2.2 Drivers and Influences on Privacy

In the remainder of this section we present a short history of the Data Protection Directive 95/46/EC and illustrate a range of developments that are presenting challenges to its applicability. We discuss in detail the role that technology, pressure on privacy and the evolving information environment have to play, how they interact with each other and how the Directive stands up against them.

Information governance concerns the way in which the management of personal information by public and private actors is changing. The protection of privacy is coming under strain due to the increasing availability and ability to process large quantities of data; the growing use of and demand for personal information, by the public and private sectors; how this personal information is used and its accountability and finally the way that this pressure is managed – or how people are reacting to this pressure. Finally technology presents opportunities to use and abuse personal information in many ways. These three factors all drive and influence each other, serving to alter the environment for the implementation of the Data Protection Directive.

2.2.1 The EU Data Protection Directive: Historical Background and Current Challenges

Current privacy protection for Europeans is still principally afforded by the EU Data Protection Directive 95/46/EC, now almost thirteen years old, and the ePrivacy Directive 2002/58/EC. The basic principles underpinning these Directives have been enshrined in a number of other regulatory texts, including the Charter of Fundamental Rights of the European Union (Articles 7 and 8), the ECHR (Article 8), and the Council of Europe

Convention number 108. The Directives ensure that specific rights are granted to data subjects, while imposing important obligations and limitations to data controllers in relation to their data processing activities. Within the context of EU policy-making, the Data Protection Directive only covers processing of personal data within the context of the first pillar of European policy (i.e. policies relating to the Internal Market) rather than the 2nd (a common security and defence policy) or 3rd pillar (police and judicial co-operation in criminal matters).

While certain aspects of the Data Protection Directive have come under criticism in recent years, its principles have set the standard for the legal definition of personal data, regulatory responses to the use of personal data and other 'innovations in data protection policy'.[3] These included the clarification of the scope of data protection rules as covering any form of structured data processing (both automated and within the context of filing systems), definition of rights for data subjects, the provisions regarding sensitive personal data and establishment of supervisory authorities and the EU level Working Party.

While the Directive should not necessarily be considered backdated, it is important to realise that it was written in a very specific societal context, and that it is the result of extensive negotiations between countries with differing legal traditions. The outcome is a compromise text, containing a mixture of provisions and obligations which were almost invariably considered essential in some countries, but barely acceptable in others.

Even though the Directive was adopted in 1995 it is rooted in the period before the Internet and the information society in general were firmly established in Europe. In fact many European countries had already put data protection acts in place at the national level years or even decades before that time, such as the UK's Data Protection Act of 1984, Berlin's Data Protection Act of 1990 or France's Act of 1978 regarding informatics, files and liberties, all of which strongly influenced the notions on which the Directive is based. This is relevant, because one of the main considerations at the time of the Directive's creation was not to create a legal framework which was well adjusted to take on future data protection and privacy challenges, but rather to harmonise existing regulations and to create a common European market for the free movement of personal data. These existing regulations were thus largely created in a context where data sharing and reuse were considered threats rather than realities, and where the fear of all-encompassing electronic databases was very dominant.

The outcome of the negotiation process that resulted in the Data Protection Directive is therefore a text that incorporated elements from several legal traditions, some of which were not universally considered to be intuitive or particularly well suited to handle day to day privacy challenges. Commonly criticised elements include the creation of a general notification obligation with a central supervisory authority in each country, the definition of static roles of data controllers and data processors, and very demanding criteria for the export of personal data to third countries.

---

[3] Bennett C.J. and Raab, C. *The Governance of Privacy: policy instruments in a global perspective*; 2nd Edition, MIT Press, London 2006 p 97

Currently, the Directive is almost thirteen years old, and the social environment surrounding the creation, management and use of personal data has evolved significantly since the Directive's creation. Indeed, while stressing that the rules of the Directive were substantially appropriate and that no amendment seemed to be in order, the European Commission has acknowledged[4] that some controversies remain in its application, most notably surrounding the general notification obligation, the application of the rules on the Internet, and the increased importance of personal data exports to third countries. In contrast, non-regulatory or self-regulatory approaches are seeing increased attention: the adoption of binding corporate rules is actively encouraged as a valid complement to adequacy findings[5]; and identity management has grown into a discipline in its own right that deals with challenges such as data ownership, data stewardship and data broking at a non-regulatory level.

2.2.2 Information Governance

Contrary to the common fear at the time of the Directive's creation, of centralised control over personal data, users are now also beginning to assume a larger role in managing and re-using their own personal data. The landscape for the management of personal data is continually evolving in new ways, as a report from the European Commission Joint Research Centre (JRC) outlined.[6]

Research in the PRIME[7] project and the FIDIS network[8] has also demonstrated that the online world is a complicated new environment where structures that have evolved in the real world over time have to be established in a relatively short time. The main challenge in this respect is the creation of transparency and awareness, as many users are neither aware of the vast quantity of personal data they (voluntarily or accidentally) disseminate across public networks, nor of the potential for reuse and abuse of these data collections. More than ever, it has become clear that collections of personal data are not static: their scope, function and ownership can change rapidly, and the persons involved are not often aware of how their data can/may/will be used.[9]

---

[4] Communication on the follow-up of the Work programme for a better implementation of the Data Protection Directive (07.03.2007), p.6; see http://ec.europa.eu/justice_home/fsj/privacy/docs/lawreport/com_2007_87_f_en.pdf

[5] See e.g. Working Party document WP 108, « Working Document establishing a model checklist application for approval of Binding Corporate Rules", adopted on 14 April 2005; http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp108_en.pdf

[6] Daskala, B., Maghiros, I., *D1gital TerritOries - Towards the protection of public and private space in a digital and Ambient Intelligence environment*", , European Commission, Joint Research Centre, Institute for Prospective Technological Studies, 2007.

[7] See PRIME Project – Privacy and Identity Management for Europe - https://www.prime-project.eu/

[8] See FIDIS Future of Identity in the Information Society http://www.fidis.net

[9] See also the recent ENISA Position Paper: *Security Issues and Recommendations for Online Social Networks* ; http://enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf

2.2.3 Technological Developments

The evolving capabilities of technology represent a key determining factor in how this data is used. Technology provides the opportunity to use (store, exchange, combine, process) and abuse (commercialise, reuse in other contexts than where it was gathered), personal information in unique ways and is always evolving: what is exciting today is commonplace tomorrow. Legislation cannot always keep up with the fast pace of technological change. [10] A number of technological developments, general and specific, are important to note in the European context.

Three general technological developments are important to note in this context:

- Ongoing miniaturisation of microprocessors and increasing processor power resulting in faster automation of tasks.
- The ubiquity of high speed communications networks including residential broadband and various forms of wireless network technologies (e.g. WiMAX[11] and Bluetooth).
- Technological advances which permit the storage and preservation of vast quantities of digital information in a variety of media and in decreasing size.[12]
- (intelligent) Search technology (spiders, crawlers…) to search and structure these data collections and make them accessible.

Some other technological advances which have an acute impact upon personal data protection include:

- Personal communications devices –as well as mobile phones being a instrument for communication, the drive to convergence means that they are increasingly used as media players, games consoles, location aware devices and payment systems.[13] Thus they generate and also contain a lot of (private) information on the user's tastes, preferences, and behaviour.
- The Internet of Things[14] - combines a number of technologies to create an intelligent environment where people and objects will be communicating (or exchanging data) with and among each other. Modifications to the architecture of

---

[10] Hustinx, P., *Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council on the follow up of the Work Programme for better implementation of the Data Protection Directive* Opinions of the European Data Protection Supervisor Official Journal of the European Union C 255 27th October 2007 p 2

[11] WiMAX is a long range wireless communications protocol, similar to the 802.11 standard but applicable across a metropolitan area

[12] Coursey, D., *How MS will know ALL about you* ZDNet.com April 18 2003 available at http://review.zdnet.com/4520-7298_16-4207958.html - 1 TB of diskspace is a thousand gigabytes. In 2003 Bell predicted that such storage space would be available in 2010, yet disks of this size are available now in high street retail outlets.

[13] Miguel Helft and John Markoff 2007, "Google jumps into wireless world – It leads a drive to turn mobile phones into mobile computers", *International Herald Tribune*, 6 November.

[14] *Internet of Things 2008* International Conference for Industry and Academia, March 26-28 2008, Zurich.

the Internet such as IPv6 will enable more objects to carry their own unique electronic identification, paving the way for the inclusion of connectivity in a wide range of devices, for example, vehicles, white goods and clothing. This will be combined with the widespread deployment of sensors and Radio Frequency Identification (RFID) technology to create 'The Internet of Things'

- Web 2.0 - Social networking sites such as Facebook and 'data mashing' are examples of Web 2.0, an evolution enabled by specific technologies permitting the pooling of information from various sources (such as Service Orientated Applications) and the generation of user created content. [15]
- Electronic Identity Systems – often characterised by smart cards or biometrics, eID are becoming increasingly attractive for both the public and private sectors for applications such as access control but also persistent identity, access to travel and social benefits.

2.2.4 Pressures on Privacy

Privacy is highly dependent upon context. These contexts include the amount of information that people are prepared to give up in certain circumstances – for example more personal information may be shared between family than work colleagues. Similarly, in certain situations people may be prepared to disclose a great deal of sensitive personal information (e.g. in a medical emergency).

Related to this issue of the context of privacy is the value that may be attributed to this personal and sensitive personal information. This value can be realised, in what may be regarded from an economic perspective, as a transaction, where personal or sensitive information is released in order to gain some benefit.

The public and private sectors are exerting tremendous pressure on privacy in a seemingly endless appetite for personal information to maximise the value possible from such transactions. In the private sector; companies increasingly use personal information to better target products and services and try to establish a relationship with customers through learning key pieces of personal information. Data warehouses are mined to bring out added value from previously disparate and disconnected snippets of personal data and companies offer benefits in return for the submission of this information from potential customers.

Similarly, in the public sector, the sharing of personal data is regarded as an enabler to support the achievement of certain objectives. These include the delivery of new or existing services in a more efficient manner or the reduction in certain risks (e.g. sharing information between administrations to protect certain vulnerable groups).

The post-9/11 world has also prompted governments to collect, monitor and use personal information for anti-terrorism and law enforcement purposes[16], as e.g. demonstrated

---

[15] *Hi-Tech ways to stay in touch BBC* 7th November 2007 BBC News available at http://news.bbc.co.uk/2/hi/technology/7082566.stm

[16] E.g. see Crossman, G., et al *Overlooked: Surveillance and personal privacy in Modern Britain* Liberty; The Nuffield Foundation October 2007

recently through the Data Retention Directive[17] which also gives rise to concerns about infringement of civil liberties. Pressure for greater law enforcement power in order to meet the terrorist threat has led in some countries to greater acceptance of government monitoring and control, but it is uncertain how long this will last, as incidents of abuse may affect public perception of these policies and harm their acceptance. For now politicians and policy makers are most concerned with effective anti-terrorism policies and present this as 'finding the right balance between security and privacy',

Companies are increasingly agents of the government in some areas with regard to the collection of personal information e.g. air travel and telecommunications. This is eroding the previously clearly defined responsibilities between the public and private sectors and is an example of a situation where convergence of functions (respectively private services and public security) can lead to diminished trust and increased risk of privacy threats. Personal data is increasingly being shared without the data subject's consent, or even without any real clarity on the identity of the recipients and goals of the data transfers. Other pressures on privacy include the drive for identity management in public administrations as a way to improve service delivery to the citizen and also cut costs and national and international data sharing efforts to combat serious and organised crime and terrorism.

This appetite for personal information in both the public and private sectors increases the risk of its accidental and malicious misuse. Examples of such risks include identity theft and direct financial and personal loss to citizens arising from their personal information being made accidentally widely available and used to commit fraud. More worryingly, the ability of data controllers to correlate disparate snippets of personal data may result in more systemic social and demographic exclusion; for example, prior denial of access to health insurance due to knowledge of susceptibility to certain diseases gained from DNA or sensitive personal data.

Now that there is a greater awareness of what sorts of information can be obtained, the question of whether the pressure on privacy will ever subside becomes pertinent. The need to take measures to provide for robust data protection in the face of such pressure (which becomes heightened in times of special risk) in order to be able to balance privacy needs with security issues is thus paramount.

Approaching an understanding of some of these pressures on privacy from the perspectives of economics could prove to offer a real added value to these complicated policy issues. The incomplete understanding of the cost and price of personal data protection is reflective of an economic question, mainly the misplaced economic incentives between the private sector, the individual (who may see economic benefit from permitting use of his personal data) and the public sector.[18] This will undoubtedly be one of the central themes in reviewing the Data Protection Directive's basic principles and key provisions.

---

[17] *Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC*

[18] For a more in depth look at the role economics plays in this issue, particularly how incentives for the protection of privacy from security risks change, see Anderson R. et al, *Analysing Barriers and Incentives for*

2.2.5 Conclusion

It is thus clear that the context in which the Data Protection Directive was created has changed fundamentally. Certain basic assumptions of the Directive have been challenged, including the validity of requiring prior notifications of any data processing as realistic way of mapping such activities, the formal assessment of the adequacy of legal frameworks in third countries as an efficient strategy of achieving high levels of protection in an international context, and its conception of well defined and static purposes for data processing (e.g. in the requirement for prior authorisation). The fluidity of personal data collections has increased to a point that could not have been imagined at the time. European citizens are also becoming increasingly involved in managing their own data through social networks, which certainly constitutes an interesting avenue of control that was not envisaged by the Directive. In this way, both citizens (as users of such systems) and private sector parties (as the owners/managers) can play a more active role in managing privacy.

2.3 Ways to Protect Personal Information

2.3.1 The Current European Regulatory Regime

In a European context, the EU Data Protection Directive introduced above is an example of a regulatory instrument geared principally toward the governance of privacy. Additionally, the ePrivacy Directive 2002/58/EC provides a number of regulatory complements for the electronic communications sector. However, the Data Protection Directive remains the clear central reference text on privacy issues. Its main goal was to establish a regulatory framework that would strike a balance between a high level of protection for the privacy of individuals and the free movement of personal data within the European Union. As noted above however, the Directive is largely a compromise text, gathering influences from several different European legal traditions into a whole that can sometimes appear to be incongruous.

In order to achieve its goals, the Directive defines specific rights for data subjects, while imposing important obligations and limitations to data controllers in relation to their data processing activities.

The European regulatory framework thus embraces a number of principles with regard to personal data processing, such as the proportionality and transparency of the processing, and the limitation of the processing to specific purposes which are agreed (or at least clearly communicated) between the data controller and the data subject. The respect of these principles is possible through the definition of standard roles (most notably the data controller, processor and data subject), each of whom has specific rights and obligations under this legal framework.

This framework however takes a very static and formal approach to data processing, and as a result struggles to cope with the new privacy challenges presented in the information

---

Network and Information Security in the Internal Market for e-Communication European Network Information Security Agency http://www.enisa.europa.eu/pages/analys_barr_incent_for_nis_20080306.htm (ENISA 2008)

society. Its approach is largely based on a number of tacit assumptions which were substantially valid a decade ago, but which are much harder to apply in a society where personal data has become a fluid and mutable resource that can change form, scope and ownership overnight. These assumptions and their impact on lawful data processing will be briefly commented below.

Assumption of clear role divisions and hierarchical control

One of the central assumptions of the Data Protection Directive is that an entity either solely or jointly with others is in control of any data processing. The data controller will determine the goals and means of the processing of personal data and assume final responsibility.

However, in the current environment, the identification of a data controller becomes increasingly complicated, due to the continuously growing amount of personal data being processed and the increasing complexity of data flows. One of the consequences of this evolution is that the distinction between controllers and processors becomes increasingly blurred, and that the role of an entity evolves depending on the context. This makes the allocation of responsibilities significantly more complicated, and also means that it will be harder for a data subject to maintain an overview of the whereabouts and use of his personal data and to exercise his rights.

In summary, a key problem is that the role division as defined in the Directive is becoming increasingly dynamic, making the application of its principles difficult in practice for all parties.

Assumption of static data processing purposes and controllable information flows

In many current electronic services, information is freely interchanged, manipulated and enriched between multiple participants and for multiple purposes. In practice this is often done with little regard for the original purpose of the data, its origin, the consent of the data subjects or geographical borders. This flexibility has allowed the creation of new and advanced information systems, which bundle and re-process data to distil relevant knowledge – as can be witnessed e.g. through the increasing uptake of social networking sites and trends for 'data-mashing'. However, such practices also conflict with key provisions of the Directive, which are based on a model in which a data controller retains control (or at least an overview) over personal data and in which the data subject's consent is the main limitation of lawful processing. This model is hard to reconcile with current approaches to personal data processing, which rely on a much more dynamic and nebulous perception of personal data as an abstract resource to be mined.

Assumption of a clear distinction between identifiable and unidentifiable entities

The applicability of the Directive is demarcated by the definition of personal data as information relating to an identified or identifiable natural person. If a collection of information does not permit specific natural persons to be identified, its provisions therefore do not apply.

However, in the context of the current information society, the problem arises that the mining of large collections of (in principle) anonymous or pseudonymous information allows the creation of specific profiles, which gradually grow, extend and evolve to the

point where the identification of a specific natural person becomes possible. This is especially the case when new services (and the underlying databases of personal information) are linked together into a mesh, where the linked databases collectively result in information that can now be considered personal data.

In summary, the data collection and processing that is inherent to modern electronic environments and to convergence in general may result in anonymous or pseudonymous collections of information to naturally evolve into personal data. However, the application of the provisions of the Directive on the processing of personal data at that point is very complicated, since questions such as the consent of the data subject, identification of the original data controller and the definition of the purpose of the collected personal data are practically impossible to answer.

2.3.2 Self- and Co- Regulatory Approaches

Self- and co-regulatory approaches to privacy protection have been taken into consideration in the European perspective in Article 27 of the Directive which encourages the drawing up of codes of conduct. In order to validate such (typically sector-specific) codes of conduct, representatives of the sector can submit self- or co-regulatory texts to national supervisory authorities for verification and approval. This validation can occur at the European level via the Article 29 working party however this has only occurred in limited fashion with regard to the International Air Transportation Association (IATA) and Federation of European Direct and Interactive Marketing (FEDMA) Codes.

In a broader sense, the Safe Harbor Principles governing the export of personal data to self-certified organisations in the United States could also be considered a successful application of this self-regulatory approach, as could the increasing adoption of Binding Corporate Rules in the same context.

None the less, it has been noted "that the aforementioned legislative texts tend to regard self-regulation and co-regulation schemes as an enhancement rather than a substitute (Article 27 of Directive 95/46) means of making data protection legislative requirements more effective and legitimate[19]". This regulatory second-tier perception appears to also have resulted in a lower uptake of such initiatives in practice. This is unfortunate given the relative success of self- and co-regulatory initiatives elsewhere such as in the United States, United Kingdom and the Netherlands.

2.3.3 Technological Approaches to Privacy Protection, including PETs and Security Enhancing Measures

While the Data Protection Directive clearly emphasises a regulatory approach to privacy protection that relies strongly on the definition of rights and obligations, technological solutions have also been considered as a potential solution to enhance privacy protection. This possibility is indirectly supported by the Data Protection Directive, most notably

[19] WIK-Consult and RAND Europe: *Comparison of Privacy and Trust Policies in the Area of Electronic Communications - Final Report*, European Commission 2007 p. 10; see http://ec.europa.eu/information_society/policy/ecomm/doc/library/ext_studies/privacy_trust_policies/final_report_20_07_07_pdf.pdf

through Article 17, requiring data controllers to implement appropriate technical and organisational measures to protect personal data against a variety of risks.

The security of information systems is a fundamental obligation of the Data Controller. Article 16 of the Directive 95/46 requires the Data Controller to provide an appropriate level of security. Recital 46, which augments the meaning of Article 17, highlights the requirement that these measures should be taken both at the time of the design of the processing system and at the time of the processing itself, thus indicating that security cannot simply be bolted onto data systems, but must be built into them.

The European Commission has recently reconfirmed its interest in Privacy Enhancing Technologies (PETs) through its Communication of 2 May 2007[20], with the purpose of identifying and stressing the benefits of PETs and laying down the Commission's objectives in this field.

Thus, at the European policy level, PETs have recently been confirmed to be a possible way to improve the assurance of European data protection principles in practice,[21] although it remains to be seen to which extent actions can be undertaken by public bodies to stimulate their development and uptake in practice.

2.3.4 Enforcement Measures

Unfortunately, experience and recent studies[22] show that enforcement in practice of the principles of the Data Protection Directive (without which it remains meaningless) frequently remains problematic.

Theoretically, the enforcement mechanisms foreseen by the Data Protection Directive are relatively strong. They emphasise the role of the national data protection authority as supervisory institutions (Article 28 of the Data Protection Directive), and grant individual rights of enforcement before the competent judicial authorities to any injured parties (Article 22 of the Data Protection Directive). Thus, both the individual injured party and public bodies representing the general interest are competent to initiate proceedings to bring any disputes to a halt.

In practice however, the main method of enforcement is the initiation of investigative proceedings by national data protection authorities. Such proceedings are frequently followed by the publication of opinions or recommendations, but harder measures of enforcement including administrative or penal sanctions are rarely used. Alternative Dispute Resolution (ADR) has been considered as a potential solution to improving enforcement of privacy principles in the field.

---

[20] *Communication from the Commission to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs);* see also http://ec.europa.eu/idabc/servlets/Doc?id=28587

[21] For a practical scenario-based approach to PET enhanced electronic identification, see the 2007 *PRIME White Paper on Privacy-enhancing Identity Management*, 27 June 2007, R. Leenes ; https://www.prime-project.eu/prime_products/whitepaper/PRIME-Whitepaper-V2.pdf

[22] *Declaration of the Article 29 Working Party on Enforcement* adopted on 25th November 2004 WP 101 available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp101_en.pdf

CHAPTER 3 Research Approach

In order to respond to the questions asked by the Commissioner regarding the strengths and weaknesses of the EU Data Protection Directive, RAND Europe and its partners time.lex and GNKS Consult will use a multidisciplinary approach with a focus on foresight, taking into account in particular the strengths and weaknesses towards the coming years, rather than simply providing an assessment of what is happening today.

A literature study will provide a solid starting point for consideration, as described in the previous chapter. In two steps we will develop insights that are likely to be relevant and robust towards the future, and that will be able to inform the debate about possible revisions of the Directive based on evidence raised from literature, interviews with notable experts and practitioners in the field and a workshop in which experts and stakeholders will be confronted with possible future developments against which a series of policy measures will be considered on their merits.

This workshop represents a key part of our study. By using a scenario based workshop, characterised by certainties and uncertainties identified through the prior work, we can aim to better understand what a realistic version of the future might be, which will inform the creation of a more plausible scenario upon which to base discussion. In this way, policy actions suggested at the workshop can be carefully tailored to dealing with the potential impact upon EU privacy regulations.

As requested, the study will result in:

- identification of the main strengths and weaknesses of the EU Data Protection Directive (95/46/EC) and its application in practice and
- identification of promising avenues (both general and specific) for improving EU law in ways which will provide effective protection for individuals and society whilst minimising burdens for organisations.

The central output will be a report to be delivered to the Commissioner as a final draft by 31 January 2009, as we understand that the Commissioner is considering publication in April 2009.

Regular co-ordination and communication will be maintained with ICO staff during the study and as per the terms of the Tender, we expect comment from ICO staff on emergent themes drafts of reports and findings as the study progresses. It is envisaged that this engagement will lead to a spirit of 'shared ownership' in the execution of the study and the delivery of its outputs leading to the desired impact.

We explain the workplan below, describing the technical tools we intend to use at each phase of the study.

3.1 Workplan

3.1.1 Task 1 - Review of Evidence

The desk research will result in a state-of-the-art overview of relevant issues as currently available from the empirical evidence base at UK and European level. It will support the achievement of the first requirement in the tender for a review of the strengths and weaknesses of the EU Data Protection Directive and its implementation. There are two distinct steps in this task – beginning with a literature review. Secondly, data gathering via an open ended online-consultation and also a small number of unstructured research interviews with individuals representing stakeholders from legal and regulatory communities, data protection authorities, data controllers and processors and civil society groups will be conducted. The aim of these interviews is not consensus building but rather to identify what are the strengths and weaknesses of the Directive and explore current thinking on ideas for its improvement, to support the study team in the generation of ideas based on the empirical evidence.

3.1.2 Task 2 – Understanding the Future

The findings of the literature, survey and interviews will result in a number of issues that will be raised in a policy-focused workshop with selected stakeholders and experts. This will be loosely based on elements of RAND's 'back-casting' scenario approach.[23] The list of experts to be invited to this workshop will be agreed with the ICO prior to sending the invitations. This workshop will provide a story on the "state-of-the-art in 2015" as well as the scenario dimensions that illustrate the key uncertainties, and provide tasking to the participants with regard to measures that need to be taken today to make sure that the environment for data protection is up to a standard needed by society.

For this a scenario story will be developed as a picture of the future. This will act as 'a coat hanger' for the discussion. Development of the scenario will build upon a legacy of previous studies most notably the Living Tomorrow study conducted for Deutsche Telekom, the UK Foresight Cyber-Trust and Crime Prevention study, the eGov Vision 2020, and the scenarios developed as part of the SecurEgov study.[24] All elements that determine that future (major certainties, as well as major uncertainties) should be in it (which will have been identified in Task 1), and it should be consistent, plausible and fun. On the major uncertainties (to be explicitly identified) we will test the impact of being on different places on a scale of these uncertainties. Figure 1 below illustrates how the scenario story acts as the 'back-story' for exploration of the different uncertainties.

---

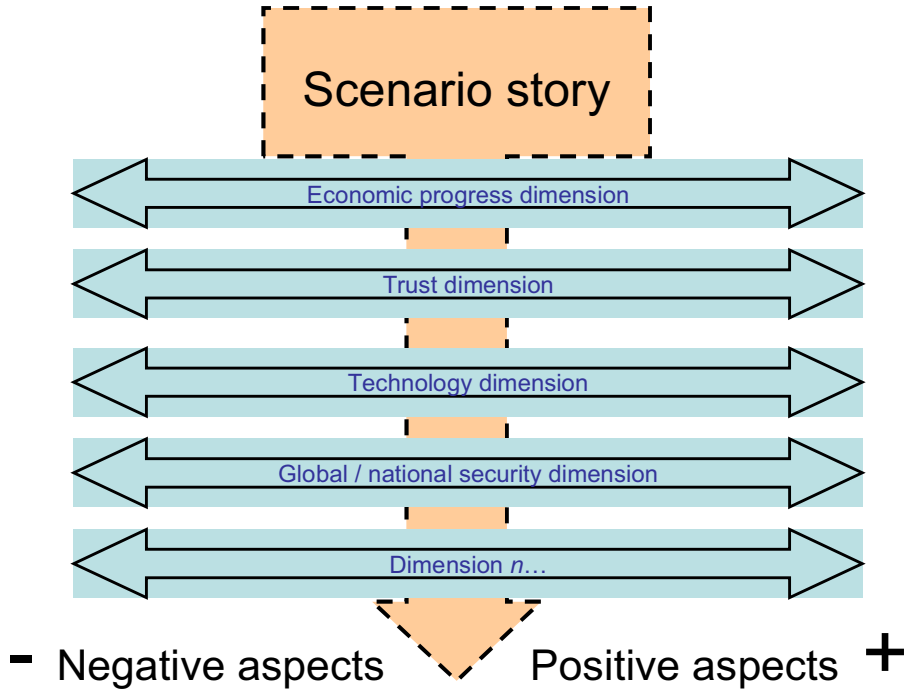
[23] For greater understanding of RAND's scenario methodology particularly the XLRM framework upon which this is based see Lempert, R., Popper, S., Bankes, S. Shaping the Next One Hundred Years New Methods for Quantitative, Long-Term Policy Analysis RAND MR1626_RPC; RAND, Santa Monica Calif 2003

[24] For a full list of recent study team projects involving scenario generation, please see Appendix B: Recent Studies

The scenario story will be presented and participants will be asked to discuss:

- What people like/dislike overall, and what threats and opportunities they see in that future (2020)
- What the positive and negative ends are for the key dimensions that matter most, and what influences the occurrence of those and determines the resulting future
- What measures should have been taken in the near future (2009-2010)

Figure 1. Scenario Methodology



Source: GNKS-Consult

The advantages of this method are that engagement of participants is easier, since only one compelling story is required (in comparison to the traditional 'back-casting approach', it permits the clear consideration of multiple dimensions and allows the knowledge and experience of participants to truly unfold since there are no predetermined extremes.

3.2 Methodology

We will use the following research tools in this task:

- **Desk Research** During the literature review phase we will use all available resources from the RAND online library, documentation and empirical evidence available to study team members along with recent work. In particular we will build upon recent and ongoing work that have bearing on this field, most notably an ongoing quantitative study using stated preference methodology aimed at understanding what drives peoples preferences toward liberty, security and privacy in a number of contexts.
- **Online questionnaire** In order to capture as many views as possible, an open-ended questionnaire will be set up available at a permanent web-link for the duration of the study, so that stakeholders can input their views and concerns into our understanding of the existing 'state of the art' regarding the strengths and weaknesses of the implementation of the Directive. This questionnaire will be based around open-ended question asking respondents to comment on what they see to be the positive and negative aspects of the Data Protection Directive as well as the practical issues they face operating within the framework of legislation derived from it. Respondents will be taken from the broad range of stakeholders that have already expressed an interest in contributing to this study.
- **Semi-structured Interviews** We will conduct a limited set of interviews with selected notable experts and stakeholders in various stages as outlined in the Research Approach. Experts will be identified from different stakeholder groups including but not limited to industry such as those companies heavily reliant upon the use of personal information but also companies trading in such information e,g. data brokers and trade associations; legal experts (both practicing and academics), policy-makers and regulators e.g. data protection supervisors at national and European level; civil society groups, academics and researchers. We envisage approximately 15 – 20 interviews which will be conducted via telephone and face to face as appropriate. Following standard RAND Europe research practice, interview reports will be made and checked for understanding with the interviewee and be subject to usual rules and procedures (e.g. obtaining clear consent in regard to attribution etc).

We will use the following methodology tool in the second task:

- **Scenario workshop** Around 30 attendees will be invited to a day-long workshop to be held at a location to be determined between the ICO and the study team (initial suggestions for it to be held in the UK - London). The scenario story and its scenario dimensions that illustrate the key uncertainties, which will have been

worked up prior to the event as a possible and internally consistent picture of the future in 2015, will be presented. Participants will be first asked to comment on the validity of the scenario to expose any inconsistencies or aspects that they consider to be unrealistic. Then they will be asked to identify the Strengths, Weaknesses, Opportunities and Threats in such a future. The rest of the day will be run according to a moderated discussion addressing the questions raised above. Participants will be encouraged to engage in debate and discussion during the day and refreshments will be provided. Further engagement will be encouraged via dissemination of a report of the day shortly afterward and, with the agreement of the ICO, offering participants the opportunity to be kept aware of progress of the study.

3.3 Deliverables

The Invitation to Tender envisages the following deliverables:

- A final report identifying the main strengths and weaknesses of the EU Data Protection Directive and its application in practice, and identifying ways of improving the law.
- Presentation of the report to the Spring Conference of European Data Protection Commissioners.
- Presentations to the ICO at key points during the life of the project.

The central output will be a report to be delivered to the ICO as a final draft by 31 January 2009 with a view to publication in final form by the Commissioner in April 2009. In order to make sure this is possible, the project team will present a full draft final report by the 7th of January 2009, expecting feedback from the ICO within one week. It is suggested that a meeting is planned towards the middle of January between the project team and ICO for a final evaluation, thus allowing the project team to finalise the report during the last two weeks of January, if necessary.

The report with its accompanying Executive Summary will be 'Quality Assured' to RAND standards.[25] Resources have been set aside for this and also for design and production to maximise the impact of the report and accompanying presentations.

Minutes of meetings and draft reports will be submitted in MS Word via email and hard copy where requested. Presentations will be submitted in Microsoft Powerpoint format.

[25] About RAND - Quality Standards http://www.rand.org/standards/

CHAPTER 4 Study team

4.1 About the Team

Members of the study team have extensive experience together working on policy relevant studies in this field both within their respective organisations and collaboratively on policy research studies. These include foresight exercises (such as the Cyber-Trust and Crime Prevention project for the UK Foresight unit) assessment of the implementation of legislation and regulation (such as the Comparative study on privacy and trust policies) and a number of studies relating to questions of privacy and identity in the future information society (e.g the PRIME and FIDIS projects). Study team members have worked collaboratively on projects concerning the generation of policy options such as the 2007 SecurEgov study and detailed legal analysis (2005 CSIRT Legal Handbook). Finally the study team can call upon experience in the application of specific research tools such as scenario development and quantitative analysis (e.g. with the ongoing RAND Europe Board of Trustees study).

4.1.1 Short Bios

Neil Robinson is a Senior Analyst at the Cambridge office of RAND Europe where he specialises in examining the economic and technical implications of information security and critical infrastructure protection. He is responsible for RAND Europe research into Information Assurance in the Defence and Security Team including research on privacy and trust in the information society. Neil is currently leading an internally funded study looking at the preferences and trade offs people make regarding privacy, security and liberty and is a contributor in the area of privacy to an ongoing project for the European Commission into the use of RFID technology in Healthcare. Neil also led the RAND Europe contribution to a 2007 study for the European Commission into a Comparison of Privacy and Trust Policies. He has worked on several advanced information assurance and security projects including a review of the Information Assurance Maturity of the UK Defence Communications Services Agency and the UK telecommunications sector, an assessment into levels of Risk Awareness and Preparedness in the EU, a Legal Handbook on Computer and Network Misuse, a Value for Money (VfM) study for the UK National Audit Office into the work of the Office of Government Commerce in the procurement of Complex IT Projects and most recently a study into Assessing the Security Challenges to the Use and Deployment of Disruptive Technologies. He holds an MSc in Information

Systems and Technology from City University, where he studied the vulnerability of the fibre optic infrastructure in London.

Prof Jonathan Cave is a Senior Economist with extensive experience in regulation, law and economics, and policy. He holds degrees from Yale (B.Sc.), Cambridge (MA), and Stanford (Ph.D.). He has led projects on telecommunications including transition from rate-of-return to price-cap regulation, legal issues arising on the electronic highway, universal service and the Internet. He has also led projects on industrial policy and government's evolving role (passing on costs of government activity to private parties, market failure in the waste disposal industry, use of government procurement as a tool to spur innovation). He works with Warwick's Centre for Behaviour under Regulation, and participates in the Industrial Economists' Network, a group composed of regulators, academics and industry representatives that concentrates on regulatory issues and the Regulatory Economists' Group. He is a member of European and British networks on Industrial Policy and Law & Economics.

Constantijn van Oranje - has master degrees in Law from Leiden University (1995) and in Business Administration from INSEAD at Fontainebleau (2000). He is Head of the Information Policy and Economics team at RAND Europe. Recent projects include: for the Independent Dutch Telecommunications and Post Regulator - a review of models for independent Telco regulators in converging markets; for the Dutch ministry of Internal Affairs - assessing the need and possible design of a Dutch Interoperability framework, and a study into the eIDM and data protection developments in the EU; for the Dutch Ministry of Economic affairs - an assessment of the policy impacts of the future of the Internet, and a policy paper on eContent policy; for the European Commission/DG INFSO - a future study on European eGovernance in 2020; a prospective view on the development of Pan European eGovernment Services; Impact assessment of the review of the Television Without Frontiers Directive; security in pan-European eGovernment - establishing the eIDM requirements for the development of pan-European services; conducting an ex ante evaluation on the impact of the Lisbon Review on Information Society policy. For DG Justice Freedom and Liberty – a support study for the impact assessment of the management of SIS II and other large scale data bases in the area of justice and home affairs; for the private sector: Deutsche Telekom - a future study on the role of ICT in society in 2015; and for British Telecom a study on defining private industry's responsibilities in the information age. Before joining RAND Europe, Mr. Van Oranje worked as an associate analyst for Booz Allen & Hamilton in London (2001-2003), where he worked on a variety of projects in ICT, and print media. Research work included a benchmarking study for the UK government on the readiness of e-Infrastructure, e-Commerce and e-Government. This was preceded by 5 years at the European Commission, working in the Cabinet of Commissioner Van de Broek (1995-1999). Mr. Van Oranje currently also advises the Dutch Foreign Ministry on European communication strategy (2003-).

Richard Warnes – Richard Warnes is a Analyst at RAND Europe, Cambridge UK. His expertise lies in the fields of Policing and Military operations and Counter-terrorism. He joined RAND in early 2007 after serving for nearly ten years as an Officer with the Metropolitan Police Service in London, including periods as a CID detective, and a

Borough Intelligence Unit desk officer for drugs and firearms. During his final three years service, he was selected to serve as a Detective in the Specialist Operations Department at New Scotland Yard, where from 2003 onwards, he participated in various covert intelligence operations and evidential investigations into terrorism within the UK. These various duties required both a thorough knowledge of law enforcement requirements for obtaining private information and their operational application, notably in relation to RIPA legislation. Consequently, he is currently involved in a major project, examining the balance between liberty, privacy and security. He specialises in research methodologies such as grounded theory and logic modelling. Prior to his police career, he served in the British Army Intelligence Corps for nine years, two and a half years full-time and six and a half years as a reservist. He saw service on peace-keeping operations during a six month posting to Bosnia during the UN and NATO phases of the civil war. Between completing his first degree and military service, he worked for seven years in international relief and human rights, travelling into Eastern Europe, the Middle East and South East Asia. He is currently a part time PhD candidate with the University of Surrey where he is carrying out doctoral research on counter-terrorism methodology in seven countries. He holds an MA in Criminal Justice Studies from Brunel University and a BSc (Honours) in International Politics from the University of Portsmouth.

Philipp-Bastian Brutscher, MPhil, is an Associate Analyst at RAND Europe. He holds an MPhil in Economics from Cambridge University, and a B.A. in Philosophy and Economics from the University Bayreuth, Germany. Philipp-Bastian has experience in empirical research methods and a good conduct of econometrics software. His research interest lies at the intersection of microeconomic theory, industrial organization, the economics of innovation and entrepreneurship. Philipp-Bastian works in the Emerging Areas Team, currently being involved in (among other studies) the evaluation of DG SANCO's Impact Assessment process and a comparative study on health research evaluation frameworks.

Lorenzo Valeri is currently a manager at the Global Technologies and Architecture Group at the Italian offices of Accenture, one of the world's leading IT management and consulting organisations. In this capacity, he advises multinational corporations and public sector organisations operating in Italy, Eastern Europe and Middle East on their information security and privacy requirements. Prior to this, between 2001 and 2006 he was a senior policy analyst first and research leader after at RAND Europe where he led over twenty public policy research projects in the field of information security, privacy and new technologies. These projects were funded by a large variety of public and private sector clients ranging from the European Commission, government departments in Germany, United Kingdom and Netherlands, Deutsche Telekom and British Telecom. Between March and September 2005, he was seconded at the Working Group for Information Security and Privacy (WISP) of the OECD where he worked in the evaluation of the information security activities of the organization's member states. Between 1997 and 2001, he was an analyst at the International Centre for Security Analysis, an independent research centre based at King's College London, where he worked in the field of information security, critical infrastructure protection and new risks to national security. He holds a doctorate on information security policies awarded in 2001 by King's College London where he was the holder of a three-year Marie Curie Research Fellowship, as well

as a research fellow in information security management issues at the Krannert School of Management, Purdue University. He has also completed undergraduate and graduate degrees at LUISS University in Rome and Georgetown University, USA. In addition to his professional activities, he is member of the European Advisory Board of the Information Security Certification Corporation (ISC2), which manages CISSP certification worldwide, and the Public Policy Committee of the Association of Computing Machinery (ACM) and sits in the academic selection board of the RSA Information Security Conference in Europe. Finally, he has been invited as a keynote speakers to leading international events and workshops organised by the OECD, ENISA, the International Data Protection Commissioners and the Dutch Presidency of the European Union. He works with RAND Europe in an independent capacity.

Jos Dumortier graduated in Law at K.U.Leuven (1973). After postgraduate studies in Nancy (Centre Européen Universitaire, 1974) and Heidelberg (DAAD, 1975), he became a research fellow at K.U.Leuven. In 1981 he finished his Ph.D. in Law with a dissertation on Private International Conflicts of Law. From 1981 to 1992 he worked part-time as a lawyer in a large Brussels law office. From 1981 until 1983 he studied Information Science (INFODOC) at the Université Libre de Bruxelles. Between 1984 and 1992 he was part-time lecturer in Information Science at the University of Antwerp. In 1985 he became a part-time lecturer and in 1993 a full-time Professor in Law and IT at K.U.Leuven. In 1990 he co-founded the Interdisciplinary Centre for Law and Information Technology and was the Centre's first Director. From 1991 to present he has been active in lecturing, research and consultancy in the area of Law and ICT, and he has published several books and articles on this subject. Prof. Dumortier is the editor of the International Encyclopedia of Cyberlaw (Kluwer International Publishers) and editorial board member of many other specialized publications. Prof. Dumortier regularly works as an expert for the Belgian federal government, the Flemish government, the European Commission and several national and international organisations on issues relating to Law and ICT. Between June 2004 and June 2006 Prof. Dumortier headed the IT law department of the Brussels based firm Lawfort, and in 1 July 2007 he co-founded the IT law firm time.lex, of which he is a partner and manager.

Hans Graux graduated in Law in 2002, and obtained a complementary degree in IT in 2003 (both at K.U.Leuven). He then joined the Interdisciplinary Centre for Law and ICT, where he did fundamental research on a number of IT law related issues, with a specific focus on electronic identity management through the ModinisIDM Study. In May 2005 he joined the IT law department of the Brussels based law firm Lawfort, where he participated in a number of international studies, specifically on the European level, including the Legal Handbook on Computer and Network Misuse, an ENISA study on risk management and risk assessment, the ELDOC Study on the cross border validity and acceptability of electronic documents, and a series of IDABC studies on interoperability in the fields of identity management, electronic signatures and electronic procurement. His expertise lies mainly in the cross border analysis of legal frameworks and policy choices, and in formulating specific policy recommendations in this field. He is also the Belgian correspondent in the FIDIS project's international survey on identity theft legislation[26].

[26] See FIDIS http://www.fidis.net/fidis-del/period-2-20052006/d51/doc/6/

Since 1 July 2007, he co-founded the IT law firm time.lex, of which he is a partner and manager.

Maarten Botterman is expert in Information Society policy issues with more than 15 years experience, with emphasis on the impact of technology, information assurance and governance issues. He is Director of GNKS Consult (GNKS stands for Global Networked Knowledge Society - www.gnksconsult.com), a company with strong associations to other research institutes and leading researchers in Europe in order to work together on policy development: making things happen. He is currently also Director on the Board of the Public Interest Registry (www.pir.org). For his work he relies on his knowledge and experience from his work as former CEO of the Information Assurance Advisory Council in the UK (2003-2006, www.iaac.org.uk) , Information Society Director at RAND (1999 – 2006, www.rand.org), as Scientific Officer for DG Information Society of the European Commission (1995 – 1999), as Senior Telework Consultant at the Dutch Ministry for Transport, Public Works and Water Management (1992 – 1995), and as Head of ICT at the North Sea Directorate of the same Ministry (1987 – 1992). He holds a degree in business economics from Erasmus University Rotterdam and is an internationally recognised expert in new methods of working and information assurance. In the past he has led the studies on Cyber Trust and Crime Prevention (www.foresight.gov.uk), on Security aspects of revisions of the European Communications Regulatory Framework, on the Development of Dependable Infrastructures (www.ddsi.org) and many others.

APPENDICES

Appendix A: Previous Studies

Relevant projects RAND Europe

Measuring trade-offs between privacy, security and liberty; 2008 (Sponsor: RAND Europe)
This internally funded study, commissioned by the RAND Europe board of Trustees, is looking at the preferences of people regarding privacy, liberty and security. It will use advantage of two main research tools –background desk research on the characteristics of some measures which have an impact upon privacy, liberty and security and a web-based stated preference exercise asking a sample of the population about their preferences in different choice contexts. The pilot will be run in June and the results are expected to be delivered by September 2008.

RFID in Healthcare (Sponsor: DG Information Society and Media, European Commission)

The objective of this study is to identify policy and research options for the European Commission (EC) to ensure large-scale, effective, and secure implementation of RFID in healthcare and the pharmaceutical market. To address these policy problems, our study will: identify the most relevant areas for the deployment and use of specific types of RFID in healthcare; analyse the potential benefits of wider implementation of RFID in healthcare; analyse the potential obstacles to wider implementation of RFID in healthcare; suggest roadmaps for the large-scale, effective and secure implementation of RFID in healthcare.

Ministry of Economic Affairs – Future of the Internet (Sponsor; Ministry of Economic Affairs, Netherlands) The Dutch Ministry of Economic Affairs asked RAND Europe to explore the critical issues arising from the emerging Internet economy, in order to inform Dutch policy makers and to help prepare for the Dutch position in the Organisation for Economic co-operation and Development (OECD) conference on the Internet in 2008. The deliverables of the study were based on a horizon scan of literature and subsequent discussion in four thematic seminars organised with two distinct groups of experts on 17 and18 October 2007. The ideas and views of the experts form the main content of the paper. However, these are supported and complemented by findings from the horizon scan and ongoing RAND studies to ensure coverage of the broad range of topics addressed by the OECD Ministerial Conference.

Comparison of Privacy and Trust Measures in the Area of Electronic Communications; 2007 (Sponsor: DG Information Society and Media-European Commission)

This project will deliver a comparison of regulatory and policy practices relating to privacy and trust in a number of countries in South East Asia as well as the United States (as both these areas have seen rapid technological as well as regulatory developments in this field).. It aims to identify the features and pros and cons of each approach for the benefit of future EU policies. This comparative exercise is understood in terms of European Commission (EC) objectives for electronic communications; including competition, the development of the internal market, and consumer rights and interests. This study is being jointly led by WIK-Consult and RAND Europe. RAND Europe is specifically delivering the analysis for the United States and India and supporting the analysis for South Korea, as well as supporting WIK-Consult in other areas, most notably report drafting and the development of policy recommendations.

Internet Self Regulation; 2007 (Sponsor: DG Information Society and Media-European Commission)

This project consists of a literature review, workshop and internal report (a Project Memorandum, or possibly a TR subject to agreement with the client for publication) for European Commission DG INFSO. The project proceeds from a review of the theory and application of current Internet regulation practices, to evaluation of their further development in existing and new sectoral schemes, as an essential stage in informing the European debate about possible future Internet regulation alternatives, in policy for 2008 and beyond. To date, the general impression that Internet co- and self-regulation may be inappropriate has lacked specific analysis. A clear exposition of the mechanisms by which problems arise and a link to available evidence could help the parties concerned by encouraging them to share more extensive data and experiences and to use the evidence to craft mutually-beneficial alternatives. A number of self-regulatory schemes relevant to identity theft are being covered in this project including those in the domain of Personal Internet Security.

BT Corporate Social Responsibility; 2007 (Sponsor: British Telecommunications plc)

RAND Europe was commissioned to write a report for BT on "Responsibility in the Digital Age" as part of its online 2007 Hot Topics series. This also forms part of BT's Social and Environmental Report for 2007. The report covered a series of general and specific questions relating to responsibility surrounding ICT companies and included specific recommendations for BT itself to act upon. The data gathering used semi-structured interviews, literature review and issues analysis along with an expert workshop where the report was validated by an international leadership panel. The responsibilities facing corporations in regard to security and privacy concerns was a key issue covered by this study.

SecurEgov; 2006 – ongoing (Sponsor: DG Information Society and Media-European Commission)

This study aims to consider what security issues surround the development of pan European eGovernment Services. The study used interviews, desk research and workshops

to gather data from a wide variety of industry, academic and public sector stakeholders on many issues relating to the management of security of an increasingly large number of public services being delivered online. Deliverables included a paper on possible Common Specifications for pan-European electronic Identity Management (eIDM) solutions and a highly regarded review of the State of the Art in electronic Identity Management.

Assessing the Security Challenges to the use and deployment of Disruptive Technologies; 2006 (Sponsor DG Information Society and Media)

This project for DG Information Society and Media focused on the privacy and security aspects of five information and communication technologies: WiMAX, Trusted Computing, VoIP, IPv6 and RFID. Next to literature analysis, each technology was further described with the means of case studies. The outcomes of the study were assessed by a panel of experts in a focused workshop and Delphi-study.

RFID Consultation workshops; 2006 (Sponsor DG Information Society and Media)

In this project, a consortium of Europe Unlimited and RAND Europe supported the European Commission by organising a series of workshop on the topic of RFID; specifically focusing on application areas; privacy, health and security; spectrum allocation and interoperability. RAND's role was specifically in preparing the discussion documents and analysing the outcome of the workshops, to be reworked into a public consultation paper.

The Information Assurance Advisory Council; 2001 – 2006 (various sponsors)

The Information Assurance Advisory Council (IAAC) is a unique partnership that brings together corporate leaders, public policy makers, law enforcement and the research community to address the challenges of information infrastructure protection. IAAC is engaged in the development of policy recommendations to government and corporate leaders at the highest levels. Our recommendations are influential because IAAC's Sponsors and Members comprise leading commercial end-users, government policy makers and the research community. For more information see: www.iaac.org.uk.

Handbook of Legislative Procedures of Computer and Network Misuse in EU Countries; 2003 - 2005 (Sponsor DG Information Society and Media-European Commission)

This project developed an easy-to-use Legal handbook covering the computer crime legislation in all EU member states for use by Computer Security Incident Response Teams (CSIRTs) and law enforcement. It also provides the necessary points of contacts in the law-enforcement community. The end product has received the praise of international organisations such as EUROPOL and Computer Emergency Response Teams (CERTs) Coordination Centre based at the Software Engineering Institute in the United States. In 2005 the Handbook is being updated and transferred into an online format. For more information see the security section of the E-Europe 2005 website at http://www.europa.eu.int/information_society/

Overview of European Information Security Policies and Strategies; 2005 (Sponsor: Japanese Ministry of Trade, Enterprise and Innovation)

This short comparative study for the Japanese Ministry of Trade, Enterprise and Innovation (METI) used semi structured interviews and desk research to provide an overview of how major UK and European public and private sector organizations dealt with the challenges of information security. This included the use of standards, technical and organisational measures and responses to legal frameworks. The study collected data on organisational structures, personnel and resources present in different public institutions charged with managing national information security strategies in a number of different countries.

NII Legal Handbook; 2005 (Sponsor US Department of Defense)

The methodological approach to the CSIRT Handbook was repeated for the US Department of Defense, in a joint project between RAND Europe and the National Security Research Division (NSRD) of RAND Corporation, applying a similar methodology to the legal frameworks of the United States (at the federal level), the United Kingdom, Canada, Australia and New Zealand.

Inventory study of EU impacts on Dutch eIDM and data protection Policy; 2005 (Sponsor: Dutch Minister of Internal Affairs)

RAND Europe was commissioned by the Dutch ministry of Internal Affairs to conduct an inventory study of all EU regulation, policies, initiatives, and projects related to IDM and data protection. The objective was to find out what EU level developments are and how they are likely to influence Dutch policies in these areas. A secondary objective was to determine how The Netherlands is performing in achieving its goals at the EU level and how other MS approach the EU. Finally the study was to present to the ministry recommendations for policies, and approaches, set against a background of global and EU specific trends. This modest study entailed in depth interviews with 10 key decision makers at Head of Unit and Director level at the European Commission and the European Data Protection Supervisor. The findings were backed up by a literature review and a global assessment of the policies in 4 selected leading countries in the area of eIDM. Subsequently these were tested and probed by a selected group of Dutch government experts from the most relevant departments, to determine how they perceived EU developments would impact their areas of competence in the Netherlands and also to see how our recommendations would apply in the political and organisational reality of their work.

Living Tomorrow; 2004-2005 (Sponsor: Deutsche Telekom)

This project for Deutsche Telekom provides an independent view of how information and communication technology developments may affect Germany as a country and society over the next decade. The study starts by highlighting social trends that are likely to emerge by 2015 due to the increasingly pervasive nature of information and communication technologies. It goes on to describe how ICT might affect family life, education, health, work, government and public life at all levels. The report concludes by highlighting what RAND believes to be social concerns that arise in Germany as a reaction

to increased integration of information technology, and what challenges need to be addressed to reap the benefits that ICT will offer in 2015. The study is based on literature interview, interviews with over 50 global thinkers in the field of ICT and a scenario exercise.

Scenarios and Gaming for Cybertrust and Crime Prevention; 2003 - 2004 (Sponsor: Foresight Directorate, Office of Science and Technology, United Kingdom)

The objective of CTCP Scenarios and Gaming is to develop scenarios and system maps to engage stakeholders in a pro-active and focused way with the implications of new technologies for cyber-trust and crime prevention. This is a step within the DTI Cyber Trust & Crime Prevention project. Input is provided from earlier activities in the project, and use will be made of ongoing DTI-sponsored networks and network activities. The activities described here will draw on the various threads in the project and provide an integrative basis for stakeholder engagement. This activity will focus on (structured) scenario based analyses and subsequent gaming. The scenario building and gaming provided a solid basis for integrating results of project activities, and a useful transferable tool for delivery to the UK Home Office at the end of the project. The methodology developed for this project is referred to as "bounce-casting": looking back from the future in order to benefit from the best of foresight and hindsight technologies. For more information: see www.foresight.gov.uk/ctcp.

Statistical Indicators Benchmarking the Information Society; 2003 (European Commission DG Information Society)

SIBIS has taken up the challenge of developing innovative information society indicators to take account of the rapidly changing nature of modern societies and to enable the benchmarking of progress in EU Member States. These indicators were tested and piloted in a representative survey in all EU member states. The SIBIS project is closely related to the eEurope and eEurope+ initiatives of the European Union and contributes to measuring the progress of eEurope actions covering all EC member states, Switzerland, the USA and 10 candidate countries. One of the areas explored was Security and trust.

Network Evolution Scenarios; 2000 - 2003 (European Commission DG Information Society)

The study for the European Commission provides an analysis of the development of electronic networks in Europe and North America and its technical, economic and political drivers. It includes four scenarios depicting possible futures of electronic networks in Europe, a framework for policy formulation, analyses of selected current policies and observations regarding possible policy measures and the input of experts and stakeholders in the field during a workshop in Brussels, and concludes with a series of observations and recommendations for policy action and further research.

The Dependability Development Support Initiative; 2000 – 2002 (European Commission DG Information Society)

The Dependability Development Support Initiative (DDSI) provides a base line on status of dependability in a wide range of countries, the related activities from a wide range of international organisations, and an action plan towards creating a dependable and secure

information infrastructures with specific emphasis on warning and information sharing, on public private collaboration and on R&D policy, from a societal development perspective. RAND Europe is the leading partner of this widely valued initiative. For more information see: www.ddsi.org.

Relevant projects time.lex

IDABC European studies on electronic authentication and multilevel security policies; (ENTR/05/58-SECURITY/SC3/) 2007 (IDABC, European Commission)

As a part of IDABC's activities in the field of interoperable e-government services management, a study on electronic identity management in secure e-government applications was recently completed with Siemens IT Solutions and Services acting as the main contractor to the European Commission, and time.lex[27] acting as the subcontractor for legal and policy matters. time.lex was requested to collect local policy information on identity management in 32 countries (27 Member States, 2 Candidate Countries and 3 EEA Countries), and to analyse this information in order to make policy recommendations. This project was recently performed for the European Commission – DG DIGIT[28] (IDABC). It was initiated in February 2007, and concluded in December 2007. The total budget of the study amounted to approximately 730.000 EUR. The study had a strong focus on the national interpretations of the concept of identity, including local perceptions of privacy and security; and on drafting policy recommendations to create a trustworthy interoperability infrastructure to allow the exchange of identity information between different administrations. In addition, this study required extensive analysis of the legal frameworks of 32 countries, including non-E.U. countries, with varying legal traditions. Thus, through this project, time.lex demonstrated its expertise for the performance of such studies. The outcome of this study has been published at http://ec.europa.eu/idabc/en/document/6484/5644.

Update to the Legal Handbook of Computer and Network Misuse in EU Countries; 2005 (European Commission DG Information Society)

This project[29] was aimed at the creation of an easily accessible overview of applicable national policies with regard to cybercrime, security incidents and applicable sanctions in the (then) 25 Member States. For each of these countries, the project team relied on a network of correspondents. The study was performed by RAND Europe, with the IT law department of the law firm Lawfort acting as a subcontractor. On 1 July 2007, this department was spun off into a separate law firm, time.lex, which is again a subcontractor in the present bid. The Legal Handbook project was performed for the European

[27] Siemens' initial partner was the IT law department of the law firm Lawfort. However, on 1 July 2007, this department was spun off into a separate law firm, time.lex, which is again a subcontractor in the present bid; and all legal obligations of the IT law department under this contract were transferred to time.lex. Thus, the contract was entirely performed by time.lex staff, and the expertise remains a part of the tenderer's background.

[28] As a part of IDABC initiatives, the Framework contract was initially signed by DG Enterprise; however, IDABC activities have since become a part of DG DIGIT.

[29] Accessible here : ftp://ftp.cordis.europa.eu/pub/ist/docs/directorate_d/trust-security/ec-csirt-d15.pdf

Commission – DG Infso between December 2004 and December 2005. The total budget amounted to 132.450 EUR. The scope, scale and methodology of this project were very similar to those of the current offer. In both cases, it is crucial that the project team has access to local experts, is able to collect valid and relevant information on the applicable legal frameworks, and is capable of processing this information in an efficient and timely manner. Thus, through the Legal Handbook project, the study team has demonstrated its expertise for the performance of projects using a similar research methodology.

In addition, all members of the time.lex team are a part of the Interdisciplinary Centre for Law and ICT (www.icri.be) of the K.U.Leuven (Catholic University of Leuven), of which prof. Jos Dumortier is the Director. As such, the team members have been involved in a number of highly relevant E.U. level research projects, including the following:

PRIME (www.prime-project.eu)

With his research team of the Interdisciplinary Centre for Law and ICT, Prof. Jos Dumortier carries out research on the legal aspects of privacy and identity management in the framework of the PRIME-project. PRIME is a research project financed by the 6th Framework Programme and the Swiss government. It aims to develop a working prototype of a privacy-enhancing identity management system and focuses on solutions that support end-users' sovereignty over their private sphere and enterprises' privacy-compliant data processing. To foster market adoption, novel solutions for managing identities are demonstrated in challenging real-world scenarios, e.g., from Internet Communication, Airline and Airport Passenger Processes, Location-Based Services and Collaborative e-Learning. As a legal partner in this project, Prof. Dumortier and his team have been in charge of the establishment of the legal requirements for the prototype and its application in the context of the selected use scenarios, and of the evaluation of the results from a legal and regulatory point of view. In the 7th Framework Programme, Prof. Dumortier and his team will continue research work on regulatory aspects of privacy and identity management in the context of the recently approved PrimeLife project.

FIDIS (www.fidis.net)

With his research team of the Interdisciplinary Centre for Law and ICT, Prof. Jos Dumortier is one of the partners of FIDIS. FIDIS (Future of Identity in the Information Society) is a NoE (Network of Excellence) supported under the sixth Framework Programme within the IST Priority in the Action Line: "Towards a global dependability and security framework". As a multidisciplinary and multinational network, FIDIS, appropriately, comprises different country research experiences with heterogeneous focuses, and integrates European expertise around a common set of activities. Additionally, all relevant stakeholders are addressed to ensure that the requirements are considered from different levels. FIDIS overcomes the extreme fragmentation of research into the future of identity by consolidating and fostering joint research in this area.

DYVINE (Dynamic Visual Networks)

DYVINE is a research project under the 6th Framework Programme. Its objective is to design, develop and test a representative version of a surveillance network based on visual sensors (images and video, in situ or airborne) which can be configured as a function of the requirements and events. This network can be used to monitor any kind of area or infrastructure which can be threatened by natural of industrial disasters. The result of the project will be advanced software module enabling the fusion of (overlapping) video data, the correlation of heterogeneous information and the tracking of persons or objects in a large area. The resulting test-bed will be demonstrated in the frame of a surveillance/disaster mitigation scenario in an urban environment. It will demonstrate real advances in Surveillance capabilities illustrating how the end-users (civil protection, cities, police, etc.) can have a global situation awareness with a large coverage and still detailed view. With his research team of the Interdisciplinary Centre for Law and ICT, Prof. Jos Dumortier, as a legal partner in the Dyvine consortium, focuses on the privacy implications of this project.

RAPID (Roadmap for Advanced Research in Privacy and Identity Management)

RAPID aimed at developing a strategic roadmap for applied research in the area of 'privacy and identity management'. The project built a robust consortium of leading experts and stakeholders and provided a forum to develop a detailed technology roadmap for R&D activities in the next Framework Programme (2003-2006) of Research and Development (FP6). The experts were drawn from industry, academic and research institutions and civil rights organisations and covered the domains of privacy enhancing technologies, IT security, law & IT and socio-economic issues. With his research team of the Interdisciplinary Centre for Law and ICT, Prof. Jos Dumortier was involved in the legal substream of the elaboration of the roadmap. The task of the ICRI was to produce an issue paper, identifying legal questions that could be further analysed in future research, taking into account socio economic and technological developments.

Relevant projects GNKS-Consult other than those mentioned above

eGov 2020 Vision study (2008)

The "2020 Vision Study: Future Directions of Public Service Delivery" aims to provide strategic advice for ICT Policy Support Programme to assist in setting its working objectives and activities for Pan-European eServices towards 2020. The project will present key trends and uncertainties that may shape delivery of public services by 2020

Assessing the impact of emerging security needs on the revision of the European electronic communications legislatory framework (2007)

This study looked at the socio-economic impact of legislation on issues like disclosure of breaches and network integrity. GNKS Consult, in collaboration with WIK (DE) and Regioplan (NL), assesses the impact of security aspects like ensuring quality of service and availability and use of location based data.