fipr

Foundation for Information Policy Research

UK INFORMATION COMMISSIONER STUDY PROJECT:

PRIVACY & LAW ENFORCEMENT

Dr. Ian Brown

University College London

Prof. Douwe Korff

London Metropolitan University

February 2004

fipr

Foundation for Information Policy Research

UK INFORMATION COMMISSIONER STUDY PROJECT:

PRIVACY & LAW ENFORCEMENT

Combined papers No. 1 & 2: Technology development and its effect on privacy & law enforcement

February 2004

CONTENTS

Acknowledgements

The authors would like to acknowledge the following people and organisations for their cooperation and advice: Advisory Panel members Richard Clayton, Eileen O'Keefe, Peter Sommer, Simon Watkin and Paul Whitehouse and members of the Advisory Council of FIPR. Phillip Webb, Kevin Robson and Fred Preston of the

Police Information Technology Organisation. Gus Hosein of the LSE and Simon Davies of Privacy International.

Parameters

This is the first in a series of papers exploring the implications of the use of new technologies for policing purposes, produced as part of a research project commissioned by the UK Information Commissioner into the question of Privacy and Law Enforcement. It describes a number of key aspects of policing in the period 1994 to 2004 and provides an assessment of likely trends and technology applications to 2009. As a means of providing continuity, these two time periods have been amalgamated into a single paper.

The paper traces the historical developments of technologies and policing over the last decade with reflections on the changing role of the police and of the relationship between the police and the individual in present-day society. The paper has specific regard to:

- The explosive increase in the generation, retention and availability of personal data;
- The practical problems of imposing constraints on data collection and retention;
- The reduction in *functional separation* between public entities (partly as a result of a drive for "joined-up Government" and increased efficiency) and the changing boundaries between the public and the private sectors;
- The absence of transparency in data collection and retention, and;
- The un-workability of the consent principle.

The second element of the research will address the likely developments in technology over the next five years, with particular regard to the growth in data relating to the relationships, transactions, personality and movement of citizens. The paper also details the development of privacy-enhancing technologies. The paper provides focus on a range of technologies and techniques, in particular intelligence data, DNA, CCTV, communications surveillance, data retention & access, ID cards; and the general increase of private-sector data on consumers that may be used by police. However, as there are a great many technologies currently in the research phase, this paper will limit itself to those innovations that are likely to be deployed at a more general level in the coming five years.

The paper provides a strong focus on the proposed changes to the police operational environment into which would be positioned a strengthened agenda for the role of communications and IT developments.

While it is acknowledged that all forms of investigative techniques and information practices will affect the rights of individuals, this paper does not comprehensively assess technologies and techniques related to forensic analysis or intrusive surveillance. It is assumed that the current oversight arrangements for intrusive surveillance provide some degree of scrutiny of such techniques. Forensic analysis is relevant to this research only with regard to the collection, storage and use of DNA and biometrics.

Summary

The UK Police service is undergoing a period of extensive change. In recent years community expectations of the service have matured, requiring a re-evaluation of the deliverables and outcome of policing. At the same time the range of policing priorities has greatly expanded, moving in the space of a decade from a focus on conventional

crime to one of preventing terrorism, preserving public order, fighting organised crime and dealing with a spectrum of computer assisted offences.

The operational environment evolving within the police service relies heavily on the expansion of IT, communications services and data. However, the adoption of more powerful and intrusive technology is giving rise to heightened privacy concerns. Personal data increasingly is available more widely throughout the service and to outside organisations. Information is often kept indefinitely. The scope of police intelligence is also becoming broader, with more categories of intimate data used in ways that a decade ago could not have been imagined.

The Formal Inquiry into the Soham murders has accelerated a trend to increased collection, storage and sharing of information throughout and beyond the law enforcement community. This has been made possible through the adoption of powerful and innovative techniques that greatly increase automation in the investigative process.

The Data Protection Act provides only limited protection. There exist few constraints on collection of data. Consent is a concept that is inherently unachievable. Disclosure and sharing of personal information is standard practice in many areas of the service. Given the burgeoning volume and use of personal information in the law enforcement community there are cogent and compelling reasons to be concerned about the practicality of the rights and remedies that are available to individuals under the law.

The police operational environment

The past decade has witnessed a significant evolution of the operational and legal environment for law enforcement in the UK. The police service and the Home Office have responded to calls for change in both the nature and the scope of policing by undertaking a range of key reforms that will ultimately influence almost all elements of police practice. Within this transformation, the role for scientific and technological developments will be of paramount importance.

Ongoing public anxiety over crime, more aggressive media reporting of police malfunction and a systemic failure of governments to deliver promised policing outcomes has required a root and branch evolution of the police service. Despite repeated commitments at a political level to improve the quality and outcome of policing, levels of reported crime have increased in many categories, while public confidence in the police service seems to have markedly deteriorated. One of the most striking features of public opinion polling in the past twenty years has been the rise in public anxiety over policing. The polling organisation MORI has observed:

> *Satisfaction with the police fell throughout the eighties, then rallied briefly before falling further in the early nineties. It then rose again to the late 90s, but has fallen steeply since. This actually seems to be fairly independent of political events such as elections, despite featuring prominently in campaigns. As a key national service we may also expect to see some relationship between views of government and views of the police. This could either be because the government is held responsible for poor police services, or a negative general view of the government leads people to be negative about one of their highest profile services - or a mixture of both of these.*[1]

A 2003 poll by YouGov indicated that the issue of crime was ranked highest as a desired priority of government. 78 percent of respondents were not confident that the police could catch an offender. 77 percent felt judges and courts are too lenient, while

[1] "The More Things Change... Government, the economy & public services since the 1970s "; MORI, 2003. Available from http://www.mori.com/pubinfo/rd/sri-change.pdf

62 percent of respondents reported that they felt crime would continue to rise.[2] Over the past decade governments have responded to such continuing concerns by introducing a range of measures designed to improve the performance and accountability of the service.

The evidence from recent inquiries into the deaths of Holly Wells, Jessica Chapman and Victoria Climbié has also been a key driver in the push for improved intelligence and more comprehensive data sharing arrangements. At the time of writing, an Inquiry into the Soham murders under the chairmanship of Sir Michael Bichard has commenced, and promises to pave the way for more comprehensive data sharing and collection provisions involving a wide range of intelligence information.

In his foreword to the 2001 White Paper on Police Reform, Home Secretary David Blunkett candidly observed:

> *Detection and conviction rates have fallen drastically over recent years. We must reverse this trend and once having established that it is not inevitable, set new targets for all those involved in the process. We must and will pick up the lessons of the research we commissioned over the summer on the average amount of time spent by police officers in the police station rather than out in the community. We must start to use technology imaginatively, not only to streamline routine tasks, but also to improve basic communication.*[3]

The government's efforts to reform the operational environment of the police service have involved a structured commitment to comprehensively engage a wide spectrum of technological opportunities. These advances are set out in general terms in both the Police Science & Technology Strategy (2003- 2008)[4] and the Forward Plan (2003 – 2008) of the Police Information Technology Organisation (PITO)[5]. These technology-based initiatives will be implemented in a broader framework of reform and organisational change that includes such strategies as the National Intelligence Model[6] and the National Policing Plan[7].

It should be noted, however, that none of these key documents provides any useful detail about specific technology developments or applications. Rather, they establish a complex business and operational framework into which can be set the specific operational initiatives. The National Policing Plan involves more than a hundred key reforms and goals, and while Science and Technology is rarely specified as a goal in itself, it is clear that the field is central to many of the other planned reforms.

The drive for structural reform

Many elements of this reform package have been broadly welcomed within the police service. There has been widespread acknowledgement that policing has in the past been handicapped by poor use of data, lack of interoperability of systems, territorial constraints and a mismatch between the utility of data and the needs of police personnel. Senior police complain that the development of large IT systems and the ease of communicating data has resulted in "information overload", spurred by a

---

2 Survey available at http://www.yougov.com/yougov_website/asp_besPollArchives/pdf/OMI030101017_1.pdf

3 "Policing a New Century: a blueprint for reform", White Paper on Police Reform, Home Office 2001. CM 5326 available at http://www.archive.official-documents.co.uk/document/cm53/5326/cm5326.htm

4 Report available at http://www.policereform.gov.uk/implementation/scienceandtech.html

5 The PIITO Forward Plan. Available in PDF format at http://www.pito.org.uk/newsroom/forward_plan/pdf/forward2003_2008.pdf

6 The Home Office. The National Intelligence Model – Providing a Model for Policing, 2000. See http://www.policereform.gov.uk/implementation/natintellmodel.html

7 The National Policing Plan. See http://www.policereform.gov.uk/natpoliceplan/index.html

tendency to risk aversion resulting in officers compiling and communicating data with little regard to its likely usefulness.[8]

Reform of the management of data has accompanied key organisational and philosophical changes to policing practices. There has in recent years been a perceptible shift toward integrated data systems and more cooperative working practices. This shift has been most apparent in the working relationships between area forces. Although the introduction of League Tables and Basic Command Units in recent years have been a contributing factor in making forces locally focused and competitive,[9] the general trend has been toward cooperation and sharing of information. The importance of a national approach to crime fighting was clearly promoted through the creation of such bodies as the National Criminal Intelligence Service (NCIS) and the National Crime Squad (NCS). The Serious Organised Crime Agency, to commence operation in or around 2006, will amalgamate these two pre-existing national agencies together with the investigation branches of Customs & Excise.[10]

The police operational and informational environment has thus moved in the past decade from regional, to cross-regional and then progressively to national. At the same time, the parameters of policing practices expanded with the development of *agency partnerships* involving non-police authorities and strategic *alliances* with private sector organisations.[11]

The Police Service and the data it envelops cannot therefore be seen as an independent organism. There is substantial support for eliminating the concept of a single "service environment". Instead, the police informational environment will in the future become fused with a vast spectrum of non-police organisations and data reserves: moving progressively from regional *unit*, to police *family*, to law enforcement *community* and finally to a full societal *alliance*.[12]

Drivers & Trends

These developments have been accompanied by two key trends. From dealing throughout their history predominately with matters of conventional crime police services moved aggressively in the 1990's to protecting public order, investing in what the European Parliament has referred to as *Technologies of political control*.[13] The second key trend is the shift to protection against terrorist activities, particularly since the attacks of 11th September 2001.

The recent changes that have occurred within the police operational environment, and the changes that are planned, are influenced by a number of drivers. These include:

- An expectation both within and outside the police service that appropriate information should be available whenever it is needed and that it should be accessible across regional borders;
- The development of "intelligence led policing" as an operational imperative of the service;

---

8 Authors' interview with Paul Whitehouse, former Chief Constable of Sussex Police, January 2004

9 *Ibid.*

10 Blunkett announces "British FBI". *BBC News Online*, 9 February 2004 Available from http://news.bbc.co.uk/1/hi/uk/3471195.stm

11 Authors' interview with Chief Superintendent Kevin Robson, Police Information Technology Organisation; February 2004

12 Authors' interview with Phillip Webb, Chief Executive, Police Information Technology Organisation; February 2004

13 An appraisal of technologies of political control. Science and Technology Options Assessment, European Commission,1997

- A general acknowledgement that police performance is inconsistent and patchy, requiring better cooperation and consistent management of operations. In 1999 – 2000 the recorded crime detection rate for burglaries varied between 43.5% and 7.9%, and for robbery between 50.8% and 14.4% at force level.[14]
- A trend to establish common data standards that allow data to be available on-demand across the full spectrum of the law enforcement community as well as throughout the family of police organisations;
- A move to proactive rather than reactive policing, resulting in a tendency to engage mass surveillance and data retention in place of traditional targeted surveillance;
- A continuing trend to establish data sharing arrangements between police and non-police partner agencies, as well as strengthening alliances between police and private sector organisations;
- An awareness that data must be not simply more accurate and reliable, but also more operationally relevant;
- A trend to organise data at a "person based" level rather than "file based" level, thus allowing disparate data to be more easily retrieved and utilised;
- A renewed effort to create an operational philosophy that is more national than regional;
- A comprehensive drive to create a nexus between police intelligence data and the "hard" data contained in the Police National Computer (PNC);
- The development of computer-assisted (and computer determined) decision-making based on available data;
- A motivation to ensure that police are able to access appropriate levels of data regardless of geographic location.

A number of these drivers have been in existence for many years, but only in the past decade have they been comprehensively mapped as formal elements of operational strategy.

Despite a clear commitment to improving the quality and accuracy of data on its systems, the police service is still failing to adequately clean the millions of files on the Police National Computer and its intelligence databases. In 2000, Her Majesty's Inspector of Police stated that:

> *Overall Her Majesty's Inspector considers the Record Type and nature of errors omissions and discrepancies found to be totally unacceptable especially given that many of these same observations were made in the 1998 PRG Report. They reflect an unprofessional approach to data quality by forces.*[15]

Despite some apparent improvements in the quality of police data, there are still indications that the process has a long way to go. When the Audit Commission investigated the accuracy of crime data in North-East Lincolnshire in 2002/03 the division was graded "red", meaning that there were "some serious problems to be

---

14 Policing a New Century. Police reform White Paper, Cmd.5326, 2001

15 K.Povey. On the Record – thematic inspection report. 2000. Her Majety's Inspectorate of Constabulary. p.142

resolved".[16] While this extent of inaccuracy continues to feature in police systems the potential threats arising from further data sharing are likely to increase.

The policing and technology blueprints

Indications of the immediate future direction of the police service are best derived from three documents mentioned earlier in this report: the *Police Science & Technology Strategy* (2003- 2008), the *Forward Plan* (2003 – 2008) of the Police Information Technology Organisation (PITO) and the *National Policing Plan*.

The *National Policing Plan* provides an overall framework for evolution of the service. Its' priorities are:

- Tackling anti-social behaviour and disorder.
- Reducing volume, street, drug-related, violent, and gun crime in line with local and national targets.
- Combating serious and organised crime operating across force boundaries.
- Increasing the number of offenders brought to justice.

The National Policing Plan established the mechanism to achieve these priorities. It is concerned primarily with such issues as management, targets, financing and accountability, but clearly states the importance of science and technology:

> *The effective use of information and communications technologies and other science and technology tools is critical if more offenders are to be brought to justice, bureaucracy eliminated to free up officers for front-line duties, and working partnerships improved between the police, the CPS and the courts. Appropriate technologies and tools include DNA, ANPR, Airwave (the new police radio communications service) and the Case and Custody system, all of which should be central to a force's science and technology strategies.*[17]

The Science & Technology Strategy takes this commitment forward with a framework for priorities within the Forensic Science Service, Police Scientific Development Branch (physical science technologies such as non-lethal weapons) and the Police Information Technology Organisation (PITO). Combined, these documents inform local police planning and they establish priorities for technology investment. A total of £285 million was spent on national police science and technology projects over 2001/2002[18] and the government has signaled repeatedly that this expenditure will continue to be supported:

> *The five-year period covered by these plans will see the most significant re-equipment programme in the history of the police service. The programme, built on foundations laid in previous years, is national in scope and embraces cutting edge IT and communications technology being applied across the spectrum of police capability needs. This complex and challenging undertaking offers major operational and business benefits to the police service and to the wider criminal justice community. This will be achieved through the effective and efficient collation, communication and presentation of information. In a nutshell, our focus is 'delivering superior knowledge at the point of decision'.* [19]

---

16 Soham probe told of police flaws. BBC News Online, 17 February 2004. http://news.bbc.co.uk/1/hi/uk/3496921.stm

17 Section 3.26 at http://www.policereform.gov.uk/natpoliceplan/chapter3_npp_plan.html#effectiveusesciencetech

18 PITO Forward Plan; p.18

19 Ibid.

Much of the work will involve extending the efficiency and functionality of existing technologies. The PITO document explains:

> *Identification services provided by PITO for finger and palm prints are poised for a major upgrade, which will improve crime detection rates attributable to this technology. Automatic Number Plate Recognition (ANPR) systems, linked to the Police National Computer (PNC) for immediate identification of stolen or wanted vehicles, are being widely deployed. Over the period of our plans the prospect is that we could further inhibit the free use of the roads to criminals. Work on other biometric techniques for personal identification, including facial recognition, is maturing and offering a fresh approach to the detection of offenders.*

The PITO plan echoes commitments made in other Blueprint documents:

> *The police service is evolving an integrated approach to its information infrastructure. It is important that this is undertaken in a way that assures the availability and integrity of systems and data. PITO is already working closely with the Cabinet Office, Communications-Electronics Security Group (CESG), forces and commercial partners to achieve this end. (...) The IT support needed to enable 'intelligence-led policing' will have been defined, developed and deployed to forces*

The reforms involve not only considerable changes in the police structure, but also a vast investment. Airwave, which will form the common communications platform for all forces, has cost around £3 billion. An indication of the challenge facing the new reforms can be gauged by how much effort was required to establish this high capacity secure radio network because not every force recognised its importance and therefore refused to cooperate.[20]

The technological environment

The evolution of information technology and analysis techniques has transformed the face of many aspects of modern policing. A combination of rising concern over crime, a widening spectrum of criminality and pressure on policing resources has generated substantial investment in research to improve decision-making and information management. The new generation of technologies create what could be described as a symbiosis between police and data systems. In this new relationship the role of the police operative is significantly changing:

> *Surveillance systems of all kinds are increasingly automated. The human component is being limited to construction and evaluation roles, with decision-making carried out by computer software through mathematical codes: digital algorithms.*[21]

It can be difficult to predict the long-term progress of technology, but five years is a realistic timeframe over which to extrapolate from existing trends. Any truly novel technology that emerges during that period is extremely unlikely to be affordable in the short term on any significant operational scale.

The last decade has seen steady increases in computing power, storage, communications capacity and coverage. The drivers behind these increases should continue over the next five years. The resulting improvement in the capacity to gather and analyse information will be complemented by an improved understanding of that data's meaning through better data mining techniques and further advances in knowledge of the human genome.

---

[20] Authors' interview with Paul Whitehouse, former Chief Constable of Sussex Police, February 2004

[21] David Wood. The Evolution of Algorithmic Surveillance and the Potential for Social Exclusion, 2003. Available from http://www.ncl.ac.uk/guru/utddprojects.htm

The Home Office has an ambitious strategy to take advantage of these increases in capability. It is aiming to support and utilise long-term advances in order to "provide capabilities far beyond those available with current technologies".[22] In cooperation with the Department for Trade and Industry (DTI), funding is being made available to encourage the UK's science and technology research base to focus its attention on reducing crime.[23] The DTI's Engineering and Physical Sciences Research Council is working with the Home Office in a £20 million crime reduction and prevention research programme from 2002—2006[24]. This means that the technology advances outlined in this report are likely to start having an impact within the next five years, and will certainly be playing an important part in police planning by 2009.

Computing power

Gordon Moore, co-founder of Intel, predicted in 1965 that the complexity per size of integrated circuits (chips) would double roughly every 18 months for at least a decade[25]. So far, Moore's law (as it has become known) has held for almost 40 years. Circuit designers believe that it should continue to hold until at least 2010[26].

In practice, this means that the computing power of chips will continue to double around every 18 months for the next five years, leading to an approximate ten-fold increase in processing power during that time. This will allow some of today's computing tasks to be performed much more quickly, although this functionality will be limited by other computer components (such as memory and storage speed) that are unlikely to achieve corresponding increases in performance.

Improvements in computing power will however allow equivalent tasks to be performed by much smaller devices at similar speeds. These advances will also open up new ways of analysing data such as searching for patterns or making inferences in large databases. Search techniques that are currently only available to top-end investigations may become available to more routine operations throughout the police service.

Storage

Data storage devices have been increasing in capacity even faster than computing power. The capacity of underlying recording media has been roughly doubling in size by area every 12 months[27]. This should continue over the next few years, leading to an approximate 30-fold increase in capacity over five years. The price of storage has now dropped to the point where it has become at most a secondary cost-factor in large systems.

Such a large increase in storage space not only allows the creation of greater reserves of data, but it will also facilitate the retention of more precise and finely grained levels of data (e.g. higher resolution and frame rate video).

Increased storage capacity will also make possible the retention of entirely new types of data. The UK "Memories for life" research challenge, for example, has proposed a system that would store and index users' "digital memories" – photographs, videos

---

22 Police Science & Technology Strategy, p.8

23 Department of Trade and Industry Foresight Crime Prevention Panel. Turning the Corner. 2000

24 See http://www.epsrc.ac.uk/ContentLiveArea/Downloads/Adobe%20Portable%20Document%20Format/EPSRC%20Briefing%20Note%20Number%20Five.pdf

25 Gordon E. Moore. Cramming More Components Onto Integrated Circuits. *Electronics*, April 1965. Available from ftp://download.intel.com/research/silicon/moorespaper.pdf

26 Shekhar Borkar. Getting Gigascale Chips: Challenges and Opportunities in Continuing Moore's Law. *ACM Queue* 1(7), October 2003. Available from http://doi.acm.org/10.1145/957717.957757

27 Andreas Moser, Kohji Takano, D. T. Margulies, M. Albrecht, Y. Sonobe, Y. Ikeda, S. Sun and E. E. Fullerton. Magnetic Recording: Advancing into the Future, *Journal of Physics D*, vol. 35(19):PR157-67, October 2002. Available from stacks.iop.org/JPhysD/35/R157

and communications – over their entire lifetime[28]. The US Government's *Defense Advanced Research Project Agency* (DARPA) proposed to fund prototype portable computing systems that would record everything that their users see and hear: a continuous multimedia diary that could be played back years later:

> *Visual, aural, and possibly even haptic sensors capture what the user sees, hears, and feels. GPS, digital compass, and inertial sensors capture the user's orientation and movements. Biomedical sensors capture the user's physical state. LifeLog also captures the user's computer-based interactions and transactions throughout the day from email, calendar, instant messaging, web-based transactions, as well as other common computer applications, and stores the data (or, in some cases, pointers to the data) in appropriate formats. Voice transactions can be captured through recording of telephone calls and voice mail, with the called and calling numbers as metadata. FAX and hardcopy written material (such as postal mail) can be scanned. Finally, LifeLog also captures (or at least captures pointers to) the tremendous amounts of context data the user is exposed to every day from diverse media sources, including broadcast television and radio, hardcopy newspapers, magazines, books and other documents, and softcopy electronic books, web sites, and database access.*[29]

This LifeLog programme had expected results within 24 months. However, after much political controversy over its parent *Total Information Awareness* program, it was defunded in September 2003 by a sceptical US Congress.[30] More information is contained in our second report in this series of papers: "The use of new technologies for policing purposes".

More prosaically, vast quantities of disk space encourage users to keep large amounts of personal information (such as old e-mail messages, documents and digital images) that they would have previously been forced to delete. The facility also allows software such as web browsers to keep large caches of visited Internet pages, providing a detailed record of every page the user has even glanced at over a period of weeks or months.

Cheap storage means that in practice, companies rarely have a pressing economic reason to delete old files. It is much cheaper to buy new disks than to identify personal data that should no longer be kept and which should be either deleted or anonymised in all of the places where it is stored (including backups). This is particularly the case when systems are upgraded and older data files may thus no longer be readable using an organisation's upgraded system. Given current evidential and forensic procedures it is likely that governments and courts will allow the police to access these reserves of personal data.

Even when files and records are deleted, most computer systems simply mark the data as deleted but leave it in place until it is overwritten later with new files. This means that any search of a hard disk may reveal personal information that is several years old.

Some legal scholars have suggested that the delete key really should mean delete, rather than merely creating the illusion of invisibility. Such a notion appeals to our sense that a momentary lapse should not permanently stain a person's record:

> *None of us is perfect. But the preservation and persistence of evidence of our imperfections does not prove we are wrong, vile, venal, or even duplicitous. It*

---

28 Andrew Fitzgibbon and Ehud Reiter. "Memories for life" – managing information over a human lifetime. Grand Challenges in Computing workshop, May 2003. Available from http://www.nesc.ac.uk/esi/events/Grand_Challenges/proposals/Memories.pdf

29 See http://www.darpa.mil/ipto/programs/lifelog/

30 See http://www.wired.com/news/privacy/0,1848,62158,00.html?tw=wn_polihead_3

just proves we are human – perhaps even farther beneath the angels than we might have wished – but lower nonetheless. [31]

From the perspective of personal privacy there is a clear threat from the access by investigative authorities to large reserves of accumulated personal data. Such reserves should be either minimised or provided with stringent legal or technological protection. However, UK legislation has if anything moved in the opposite direction. The *Anti Terrorism, Crime & Security Act 2001* provides for mandatory warehousing of records of telephone and e-mail correspondents, website visits and mobile phone location, while Part I chapter II of the *Regulation of Investigatory Powers Act 2000* allows a large number of central and local government officials to access this data (see section below on Communications Data Retention & Access).[32]

Increasing disk capacity will also make it feasible to store current data that will only become useful or possible to analyse in several years time once other information has become available. This will be more important at the intelligence end of law enforcement, where very large data sets may be amassed in the expectation that they may subsequently become useful. Two such examples are the proposal for retention of seven years of communications data suggested by a group of UK intelligence and law enforcement agencies in 2000 to allow the retrospective investigation of communications involving terrorist suspects and serious criminals,[33] and the recent law in Italy establishing a mandatory five-year retention regime.[34] More raw computing power will also be available at that later date, although this facility will not necessarily improve the quality of analysis.

Online, log-able access to information

Since the early 1990's the World Wide Web has facilitated a vast improvement in information access. It has quickly grown to contain more information than even the largest national reference libraries.

What before might have taken a trip to a library to discover – details on sensitive medical conditions such as HIV, perhaps – can now be accessed from what seems like the privacy of a home computer. In just a few years, it has become quite unusual for information on a specific event or topic to be missing from the Web. The majority of newspapers and magazines have also made some or all of their articles available online.

From a privacy perspective, the key difference between accessing information online as opposed to paper-based information lies in the potential for tracking such access. It is trivial for Web servers to record a range of information every time a specific page is accessed, including the Internet address of the computer requesting that page.

Internet access has now reached 50% of UK homes[35], while 59% of Britons over the age of 14 are users – including 98% of schoolchildren[36]. The government believes that by the end of 2005 every UK community will have access to broadband Internet connections, and is planning to announce a new target to further increase access for

---

31 James M. Rosenbaum . In Defense of the DELETE Key. 3 *Green Bag* 2D 393, 2000. Available from http://www.greenbag.org/rosenbaum_deletekey.pdf

32 For a detailed discussion of the potential privacy threats from retention see: Caspar Bowden. CCTV for Inside Your Head. Computer & Telecommunications Law Review. 2002, issue 2. http://www.apc.org/english/rights/europe/eu/cctv_for_the_head.html

33 Roger Gaspar. Looking to the future: clarity on communications data retention law. Submission to the Home Office, 21 August 2000. Available from http://cryptome.org/ncis-carnivore.htm

34 See Electronic Frontiers Italy, 24 January 2004 http://www.alcei.it/english/actions/crimprev.htm and for background read Phillip Willin: "Red Brigades ensnared by communications technology" IDG News Service (Rome Bureau) Rome. 11/13/2003

35 Oftel's Internet and Broadband Brief, 10 December 2003. Available from http://www.ofcom.org.uk/legacy_regulators/oftel/oftel_internet_broadband_brief/#1

36 Oxford Internet Survey, September 2003. Summary available from http://users.ox.ac.uk/~oxis/enough.htm

the second half of the decade[37]. New information services such as television over broadband will play an important role in these plans, and will be capable of recording much greater detail on their users' activities than would be the case with traditional broadcast television.

The police have shown continued interest in being able to access detailed records of the information retrieved by Internet users. It was only a last-minute amendment to the *Regulation of Investigatory Powers bill* that prevented self-authorised law enforcement access to the list of full Web addresses visited by an individual. These addresses give the exact page read, as well as potentially sensitive information such as the search terms entered into a Web search site such as Google or other information provided to Web sites. The *National Criminal Intelligence Service* again pushed for this full access in a submission to the Home Office in August 2001.

Digital television – via satellite, cable and terrestrial broadcast – is also a significant and growing source of entertainment and information for UK citizens. The set-top boxes used to access these services are typically powerful computing systems that are able to record a great deal of detail about their users' viewing habits, which can then be communicated back to the service operators for marketing purposes.

It is likely that third generation mobile phones will make up the majority of new Internet access devices. They have been slow so far to take off, but will become pervasive as their price drops and as previous services are phased out. Higher connection speeds and better screens will enable access to a much greater range of content. As 75% of British adults already own a mobile phone[38], this evolution will present a potentially far more popular platform for Internet access than the personal computer.

Set-top boxes and mobile phones are generally not programmable by their users in a way that allows the deployment of Privacy Enhancing Technologies (see the chapter later in this paper). Because of the marketing utility of records of information that have been accessed, there is not a strong economic incentive for service providers to add such facilities to their technology. Information on the content accessed by users could prove to be a valuable way to target online and offline advertising as well as being a valuable reserve of data for investigators.

Bandwidth and wireless connectivity

The growth in capacity and coverage of communications links continues to provide a spur to the networking of surveillance devices. Wireless links allow microphones, still cameras and video cameras to be connected to wired networks without the need for fixed cabling to be installed. Video and audio may then be cheaply carried to any other point on the network.

Since the arrival of the mass market Internet in the early 1990's the marginal cost of transporting data has dropped dramatically. Data transmissions no longer need to tie up expensive phone or leased lines that are charged on a per-time basis. A vast amount of transmission capacity was installed during the dot.com boom, and will be available at a low price for some years to come. Advances in Dense Wave Division Multiplexing technology[39] will continue to increase the amount of data that can be transmitted within telecommunications companies' networks using existing fibre optic cables.

A range of faster radio access technologies are becoming available to connect devices in and around homes and offices to these networks without the need for expensive re-

37 Richard Wray. Broadband target to be election pledge. *The Guardian*, 21 January 2004. Available from http://www.guardian.co.uk/online/news/0,12597,1127512,00.html

38 Oftel Market Information: Mobile Update, October 2003.

39 A technique that can transmit many streams of information through one fibre optic cable using different light wavelengths.

cabling. They provide wireless connectivity with ever-greater rates and coverage. To put the following figures in context, a reasonable quality video stream only takes up around 1Mbps (megabits per second):

- High-speed Wi-Fi networks are becoming common in urban areas. The current standard provides 11Mbps communications, and a new version provides 54Mbps[40].
- Third-generation mobile phone networks, after a slow start, are likely to provide access at 2.4Mbps with similar levels of population coverage of the country as existing mobile phone networks within five years.

Mobile phone cameras have been a huge success and have already been adapted into surveillance devices. Nokia's Observation Camera, for example, will send a photo of the area it is focused on to any mobile phone that supports picture messaging, and can be triggered by a text message, time interval or built-in motion detector[41]. It can be placed anywhere within range of a mobile phone network and power supply.

These factors mean that the trend towards surveillance devices being networked is likely to accelerate. High-quality video footage from CCTV cameras, for example, could be gathered at central transmission points in a building and then carried over the Internet to any destination at very low marginal cost. Lower-quality video can be relayed from anywhere within range of a mobile phone network. This will reduce the costs of setting up CCTV networks, encourage the use of more cameras, and allow higher levels of off-site processing (such as storage or image recognition). It will give law enforcement agencies the ability to put an increasing area of public space under visual surveillance. With the cooperation of system operators, the technology will also provide access to surveillance systems covering a greater number of private spaces.

West Midlands police, for example, have installed:

> *[A] high-speed broadband Wan [that] enables key stations to communicate at greater speeds and share critical information in a secure environment.*
>
> *The infrastructure can… handle video streaming from helicopter-mounted cameras and high street CCTV systems*[42].

Data analysis capability

It is relatively easy to search through large datasets for a specific item such as a particular rendering of a name or phone calls made to a particular number (see the section on communications data below for more information on the latter). This can provide large quantities of data in response to a specific request. But even at this simple level, intelligence data about a threat may not be capable of deducing such exact search terms. Widening the search to include common variants of names, a larger range of addresses etc. may result in too many pieces of data matching the search criteria to be usefully examined.

The type of problem this can cause is shown by experience with the terrorist watch lists searched by airlines as they check in passengers within the US. To prevent different spellings of a name from being missed – a particular problem where non-Roman names have been transliterated into English – many airlines use a sound index to match similar-sounding names. However, this has caused thousands of

---

40 Richard Shim. 802.11g: Final testing begins. *CNET News.com*, 26 February 2003. Available from http://news.zdnet.co.uk/hardware/mobile/0,39020360,2131095,00.htm

41 http://www.nokia.com/nokia/0,,4654,00.html

42 Ross Bentley. Police chase high-speed connectivity for voice and data traffic across the Midlands. *Computer Weekly*, 27 May 2003. Available from http://www.computerweekly.com/Article122008.htm

people with names similar to those on the lists to be stopped and questioned at airports. As the San Francisco Chronicle recently commented:

> *In their efforts to prevent a repeat of the Sept. 11 tragedy, the U.S. government and the airline industry are relying on software so outdated that it can't distinguish between the last name of terrorist mastermind Osama bin Laden and punk rocker Johnny 'Rotten' Lydon.*[43]

This is an active area of research, with many very much more sophisticated methods of name matching having been developed[44]. However, because of the nature of intelligence-gathering, there will continue to be circumstances in which the police need to search for information on suspects with correspondingly inexact information such as possible spellings of names or pictures from a poor-quality photograph. It will always be difficult to avoid a high percentage of false positive results when a large database is being searched for a small amount of inexact data.

High quality data is an important pre-requisite for high quality search results, as well as being a key goal of data protection. But this can be a problem in intelligence databases that often store unverified information from single sources. There exists no comprehensive audit of the accuracy of police intelligence systems,[45] but an audit of data transferred to the Police National Computer by the Metropolitan Police Security Inspection Unit found a substantial error rate, which would obviously make accurate searches difficult[46] and could cause numerous problems for someone who was incorrectly identified as a criminal suspect. The reliability of information on police intelligence systems may also diminish as those systems are fed with an increasing mass of intelligence data.

Profiling an individual – linking all of the information known about that person in one or more databases – is again relatively easy but is dependent on the quality of the dataset. Errors in the spelling of names, classification of individuals or other variables can cause potentially important data to be missed from a profile, or mistakenly included in another individual's profile. This is less the case when a number of pieces of information are being matched against a profile. But the situation is not aided by the current police practice of collecting data according to file and case, rather than through a person-based index. Some police believe these tasks will be made easier with a national ID card number (see later section).

The Police Science & Technology Strategy envisions that enhanced data matching and information sharing will be used to introduce further profile information.

Far more sophisticated data analysis procedures exist, and are heavily used in the marketing and financial industries on large-scale datasets. These have gone beyond simple statistical techniques to using techniques inspired by the natural world. Artificial neural networks work in a conceptually similar way to the action of a large number of highly interconnected neurons in the brain, and have proven to be adept at learning to recognise hidden patterns in data. The performance of genetic algorithms is increased by combining and mutating trial algorithms, selecting the "fittest" results and repeating the process. Both are used to find patterns that will indicate likely responders to advertising campaigns or fraudulent credit card transactions. They have had particular law enforcement applications in facial recognition (see the later section on CCTV in this paper) and are being investigated for use in the Computer-

---

43 Alan Gathright. No-Fly List Ensnares Innocent Travelers. *San Francisco Chronicle*, June 8, 2003. Available from http://www.commondreams.org/headlines03/0608-03.htm

44 For one recent comparison of algorithms, see: W. W. Cohen, H. Kautz, and D. McAllester. Hardening soft information sources. In *Proceedings of the Sixth International Conference on Knowledge Discovery and Data Mining*, August 2000. Available from http://www.cs.washington.edu/homes/kautz/papers/dmac-cohen-kautz-kdd2000.ps

45 Authors' interview with Kevin Robson, PITO, February 2003

46 Mike Simons. Errors rife in police data file. *Computer Weekly*, Thursday 27 April 2000.

Assisted Passenger Pre-screening System II in the US (see the second paper in this series of reports).

But searching out patterns pointing to serious crime is a difficult type of analysis. It will normally involve searching for a very small number of occurrences of a certain pattern amongst an enormous volume of data. Such searches are difficult to tune in such a way that they identify patterns of interest without also returning in a large number of false positive results (mistakenly matching individuals with the selected patterns). These false positives can have more serious consequences than the generation of an irrelevant advertising letter, potentially leading to police inquiries into a misidentified suspect. One leading security expert has commented:

> *Relying on computers to sift through enormous amounts of data, and investigators to act on every alarm the computers sound, is a bad security trade-off. It's going to cause an endless stream of false alarms, cost millions of dollars, unduly scare people, trample on individual rights and inure people to the real threats.*[47]

The quality of these searches can be improved by trying to find relations within data, such as hypothesising that a group of criminals will tend to call or e-mail each other or share previous addresses. Members of such related groups can then be examined more closely. But this assumes that criminals will not learn to avoid generating this relational data (for example, by using multiple pre-paid mobile phones in different patterns) or cause spurious data to be generated[48]. Many criminals will not, but the sophisticated ones who would be most proportionately targeted using this technique are perhaps likely to do so. The technique is also of little use with volume crime, where criminals tend to work alone.

Nor is it clear that such analyses would enable investigators to find and stop criminals before they commit serious crimes, even with access to very large amounts of information in government and private sector databases. However, once such a system was built, it would be difficult to stop the addition of ever more data for analysis. Any privacy rules that were put in place would be vulnerable to being removed if there was a perception at a later point that they were reducing the effectiveness of the system.

The use of intelligence tools to analyse and profile communications and other data is now commonplace in most investigative agencies. The potential they offer is tantalising:

> *[R]apid advances in computing power now permit warehousing and "traffic-analysis" of unlimited quantities of communications data by automated tools that derive "friendship trees" and can detect patterns of association between individuals and groups using sophisticated artificial intelligence programming. This method can be considered as a "suspicion-engine" which can identify new targets of investigation with complete generality – without any access to the content of communications – but which could subsequently serve as the basis for an interception warrant.*[49]

This paper later discusses some of the specific intelligence analysis tools used by the police. Many of the technologies and operating techniques tend to resist the data protection principles relating to necessity, proportionality and time limitation.

---

47 Bruce Schneier. *Crypto-gram*, January 2004.

48 David Jensen, Matthew Rattigan and Hannah Blau. Information awareness: a prospective technical assessment. *Proceedings of the ninth ACM SIGKDD international conference on knowledge discovery and data mining*, August 2003

49 FIPR briefing to the House of Lords, 2000. Available from http://www.fipr.org/rip/FIPR%20Lords%202nd%20reading%20briefing.htm#_ftn7

Specific classes of technology

Most technology advances in policing over the past decade and that are scheduled in the next five years are concerned with one or more of five principal aims:

- Ensuring that communications and data transfer can occur interoperably at a national level and in a fashion that is secure and reliable;
- Ensuring that means are found to correctly identify and locate individuals;
- Providing a means to diminish the *mobility* and *invisibility* of suspects;
- Establishing a timely, accurate, speedy and more cost-effective means of processing intelligence data and forensic material;
- Deploying techniques that can aid in the decision-making process.

The applications that have been pursued are many and varied. They fall roughly into the following categories:

- *Database* technologies that store personal information;
- *Analysis* tools that process this information for a range of investigative purposes;
- *Communications* technologies that permit the transmission of data;
- *Identification* techniques that attempt to uniquely identify individuals;
- *Tracking* technologies that aim to locate or follow a target;

Appendix 3 of the Science and Technology Strategy lists around 70 technologies, techniques and projects that have a bearing on the rights of data subjects. Amongst the most obvious of these are remote vehicle tracking, dynamic face recognition, portable biometric and DNA testing devices, thermal imaging, use of DNA to predict physical characteristics and active and passive tagging.

The Strategy outlines some key deployment goals for the coming five years. These include:

- *Airwave, the new digital communication system being rolled out to all forces.*
- *Development of seamless and secure information processing across the Criminal Justice System.*
- *The national DNA database, being expanded to cover the active criminal population.*
- *Wider deployment of ANPR (Automatic Number Plate Recognition) technology across the service to target known offenders.*

The Science and Technology Strategy also prioritises a number of technology developments, many of which involves significant and fundamental data protection aspects:

- *Automated and miniaturised equipment to allow the speedy analysis of DNA and other processes at crime scenes, a 'lab-on-a-chip'.*
- *Technologies with surveillance applications such as passive millimetric microwave.*
- *Information Systems, including new national databases (e.g. firearms and persistent offenders).*
- *Portable 'Livescan' fingerprint scanning systems.*
- *The evaluation of mobile data entry systems in policing applications.*

- *Further development of Biometrics – including face and voice recognition.*
- *Research on DNA – identifying offender characteristics from DNA.*
- *Cell Type Analysis – to determine the origin of cells (e.g. hair, skin).*

Major data resources

The Police National Computer (PNC)

The PNC was established in 1974 to provide a central resource for police to identify and trace stolen vehicles. Since that time it has become the key resource for law enforcement information across the UK "to support the police in exploiting information held anywhere within the police domain".[50]

The PNC holds around 50 million records on more than six million UK citizens, together with details of registered drivers. The data also includes fingerprints, photofit pictures, DNA flags and details of missing and wanted persons. Almost 500,000 enquiries are received by the system each day[51] via 10,000 terminals located within police organisations and other law enforcement agencies, security services, the Criminal Records Bureau, HM Customs and Excise and other non-police organisations. In the year 2001 to 2002, PNC use increased by more than 10 per cent over the previous year.[52]

The PNC predominately contains what the police refer to as *hard* or *factual* data, though integration with *soft* data in intelligence systems is underway. In the thirty years since its inception the PNC has grown to become a vast interactive reserve of data. The functionality and scope of the system has grown each year:

1974 *Stolen Vehicles*
1975 *Broadcast*
1976 *Fingerprints*
1976 *Vehicle Owners*
1977 *Criminal Names*
1978 *Wanted/Missing Persons*
1980 *Disqualified Drivers*
1983 *Crime Pattern (now Comparative Case) Analysis*
1985 *Convictions History*
1991 *Stolen Property, Transaction Log, Combined Directory*
1994 *Marine Craft, Firearms*
1995 *PHEONIX (Names Index)*
1996 *VODS (Vehicle On-line Descriptive Search)*
1997 *ANPR (Automatic Number Plate Recognition), Sex Offenders*
1998 *QUEST (Querying Using Extended Search Techniques)*
2001 *Motor Insurance, Jurors, FSS link*
2002 *Drivers Database, CRB link, 'Live' PNC and PNC Disaster Recovery upgrade*

---

50 PITO Forward Plan

51 During 2001/2002, more than 78 million business transactions were processed, along with a further 82 million 'fast-track' ANPR transactions. PITO Winter News 2002/2003. Available from http://www.pito.org.uk/newsroom/pito_news/html/winter2002/story10.html

52 Ibid.

***2003** MOT rollout*[53]

Among the categories of personal data held on the PNC are:

- arrest details
- details of offences and methods
- personal descriptions
- bail conditions and remands
- convictions
- custodial history
- wanted/missing reports
- disqualified driver records
- cautions
- drink drive related offences

The PNC also contains information and flags relating to a range of specialist police databases including the Metropolitan Police Service (MPS) *central index of prostitutes* and the central MPS *juvenile index.*[54]

The PNC will be further extended in the coming year with the addition of a national firearms registry and a single national Violent and Sex Offenders Register (ViSOR), shared by both the police and probation services. The PNC is also moving to full compatibility with the *Schengen Information System* (SIS) to exchange criminal and *wanted person* information across Europe. SIS is also poised for expansion to include four new categories of people: "violent troublemakers" such as protestors and suspected football hooligans, people whose visas have expired, who would be subject to arrest and expulsion, an "EU visa database" to record all visa applications (issued and refused) and a database of all third country nationals legally resident in the EU (more than 14 million people).[55]

PITO envisions a continuous enlarging of the PNC throughout the indefinite future, particularly with the expansion of fields, operational capability, access by increasing number of accredited non-police organisations and the constant development of other applications across specially designed interfaces. PITO envisions comprehensive mobile access to the PNC to be rolled out nationally in the short term. Police in Staffordshire have already been issued with GPRS-enabled laptops to access the PNC[56].

Former PNC Director John Ladley has commented:

> *We have put in place a flexible architecture to enable PNC to go in whatever direction is required of it. We have not closed any doors, but simply left a number of them ajar for future development opportunities... One thing is for certain - the PNC is going to be a very different animal in the future compared to what it is today.* [57]

---

53 See http://www.pito.org.uk/what_we_do/police_national_computer/

54 Police National Computer Bureau Homepage http://www.met.police.uk/so/pnc.htm

55 Tony Bunyan and Ben Hayes. *The Guardian*, London. September 10, 2002 http://www.guardian.co.uk/bigbrother/privacy/statesurveillance/story/0,12382,789721,00.html

56 Andy McCue . Mobile police increase time on the beat. Silicon.com, September 23 2003. Available from http://www.silicon.com/management/government/0,39024677,10006127,00.htm

57 Spotlight. PITO News, Winter 2002/2003. http://www.pito.org.uk/newsroom/pito_news/html/winter2002/story10.html

After the recent Soham murder trial, police have agreed that future allegations and reports relating to sexual offences and child abuse should be placed or flagged on the PNC.[58]

Police now consider that some data on the PNC can be stored indefinitely, in keeping with legal rulings related to DNA[59]. A "Weeding" committee within ACPO is currently considering new retention periods for various categories of data.

Intelligence analysis

The increasing amount of data available to investigations has created both a major opportunity and a major challenge for police. The potential for determining patterns of criminal behaviour and even for predicting movements of criminals co-exists with the threat of information overload.

Several software tools have become available to support investigating teams in identifying key pieces of information within intelligence and other systems. The two main categories of tools are information visualisation and data mining programs. This section describes the most popular programs used by UK law enforcement agencies[60].

Both sets of tools first require that data from disparate sources is merged together for analysis, with records concerning the same entities being identified and consolidated. Poor quality original data sets will make this process difficult.

Information visualisation

The popular *Watson* system is an intelligence visualisation tool produced by Xanalys LLC. It allows links between information gathered as part of an investigation to be displayed graphically, allowing analysts to see and further investigate patterns – such as between people, telephone calls, financial transactions and organisations:

> *In Watson, analysts construct queries about their data by using a drag-and-drop icon-based Query Editor, and then choose how they want to see the results: as a report consisting of a set of tables, or in a chart where data appears as icons connected by lines. Watson has algorithms that automatically lay out the charts in ways that allow the human eye to easily see underlying patterns; and users can override any of Watson's layout choices. For example, an analyst could apply a special icon to men in their 30s who live in a certain part of town, or highlight links between known gang members.*
>
> *Watson works quickly even with large databases, allowing analysts to expand or narrow their queries over and over again until the analysts find the information they're looking for. Analysts can examine the same query in a variety of ways—perhaps once as a report, once as a chart of connections, and again as a timeline. All three views could be on the screen at once, and a change in one chart is automatically propagated to the others[61].*

Similar tools such as Visual Analytic's *VisualLinks*[62] and i2's *Analyst's Notebook* are also widely used by UK law enforcement agencies. The latter includes a specific phone call record analysis tool, with the following capabilities:

- *Rapidly import up to 100,000 telephone call records at a time*

---

58 Martin Bright and Kamal Ahmed, The Observer, London December 21, 2003

59 Authors' interview with Chief Superintendent Kevin Robson, PITO, February 2004

60 Peter Viechnicki. Using Link Analysis to Leverage Enterprise Data. Featured article, NCCAIIM, December 2003. Available from http://www.nccaiim.org/Newsletter/2003_12_Feature_article.htm

61 Xanalys LLC. Watson Data Sheet. June 2003. Available from http://www.xanalys.com/documents/WatsonDataSheet.pdf

62 See VisualLinks web pages at http://www.visualanalytics.com/Products/VLFeatures/index.cfm

- *Identify groups of calls that repeatedly occur together and present that information in concise charts*
- *Help establish the chain of command in a criminal organization*
- *Discover the existence of unknown players and focus your investigation*
- *Predict future incidents more accurately based on historical call patterns and temporal analysis*[63]

These types of tools rely upon police analysts to search out information useful to the investigation. They can help by identifying highly-linked records, such as a small group of people that have been telephoned by a large number of persons under investigation.

Data mining

Data mining tools attempt to find more complex underlying patterns in large data sets. They are also used in a wide range of business applications but are currently less specialised than the specific law enforcement programs described in the previous section.

SPSS's *Clementine* has been used in the US and the UK by police agencies to investigate cases. It works as follows:

> *The predictive analytics process begins by exploring the way in which specific business issues relate to data describing people's characteristics, attitudes and behavior. These numeric and free-form data sets, which originate from both internal systems and third-party providers, are cleansed, transformed, and evaluated using statistical, mathematical, and other analytic techniques. These techniques generate models for classification, segmentation, forecasting, pattern recognition, sequence and association detection, anomaly identification, profiling, propensity scoring, rule induction, text mining and advanced visualization.*
>
> *When these predictive analytic models are combined with organizational knowledge, the result is insight into the critical business issues mentioned earlier. Through measuring uncertainty surrounding these issues, predictive analytics enables proactive risk management, serving as a guide for refining key decision making processes through controlled, iterative testing of potential actions and their likely intended—and unintended—consequences. These findings and their corresponding business rules can then be deployed within front-line operational systems, resulting in revenue increases, cost reductions, process improvements and competitive advantages.*

Clementine has been used by West Midlands Police to re-examine unsolved theft cases. The details stored on each electronic case file are analysed to find clusters of cases where thieves have a similar appearance or modus operandi. If clusters of physical appearances match those of MOs, it is possible that the crimes were committed by the same individual. This allows leads to be grouped and the cases reprioritised. If one case is solved, the identified individual can be questioned further about the remaining crimes[64].

Richmond, Virginia's Police Department has used *Clementine* in a similar way. It has also used the system to predict crime hotspots and deploy police officers accordingly, as well as to identify property crimes that are likely to escalate into sexual violence[65].

---

63 See PatternTracer web pages at http://www.i2inc.com/Products/Pattern_Tracer/

64 SPSS case studies, available from http://www.spss.com/success/template_view.cfm?Story_ID=14

65 Richmond (Va.) Police Department Tackles Crime With Predictive Analytics From SPSS. SPSS News, 8 January 2004. Available from http://www.spss.com/press/template_view.cfm?PR_ID=647

SAS *Enterprise Miner* is the other major data mining tool used by law enforcement:

> *SAS Enterprise Miner takes the first step by helping generate questions you might never have thought to ask. The resulting models can complement other analytical query and reporting tools. SAS Enterprise Miner's exclusive "Sample, Explore, Modify, Model, Assess" (SEMMA) approach provides users with a logical, organized framework for conducting data mining. Beginning with a statistically representative sample of your data, this methodology makes it easy to apply exploratory statistical and visualization techniques, select and transform the most significant predictive variables, model the variables to predict outcomes, and confirm a model's accuracy*[66].

Florida's Department of Corrections uses SAS software to store in-depth information on inmates and those on community service throughout the state. This information is analysed along with other databases such as those maintained by the state Department of Education and the Supreme Court. The Corrections Bureau is then able to search for patterns that would match those of crimes being investigated by local police, allowing it to suggest suspects[67].

There are some potential data protection issues that arise from the use of these analysis tools. As mentioned elsewhere in this report, no audit of police intelligence reserves has been conducted. As the use of data drilling and data mining often leads to unfounded suspicion and even subsequent investigation of innocent parties, the existence of incorrect data on these systems can result in the generation of an array of false conclusions.

The tools described above can also make use of a range of general non-intelligence databases such as the electoral roll, Post Office "Change of Address" lists and telephone number listings. With the imminent development of a common data standard between the PNC and intelligence systems, and with the establishment of the Corporate Data Model across the entire Law Enforcement community there will be substantial issues concerning the viability of data protection in the policing environment.

Customer databases

The growth in the last decade of large private sector databases on citizens has been one of the notable consequences of the increase in data storage capacity and computing power. Police are anxious to access such data, particularly as private sector *alliances* on a range of issues from art theft (insurance databases) to bank fraud (credit reference databases) are created in respond to demands for improved investigation.

In an effort to improve their profitability companies now store and analyse large quantities of personal information. However this data is also available to the police under procedures such as section 29 of the *Data Protection Act 1998,* and it is a key component for analysis by the Total Information Awareness-type schemes described in the second report in this series of papers.

Police use of commercial data reserves has increased over the past decade, and has been more pervasive since the events of 11 September. Professor David Lyon has observed:

> *One of the ways in which surveillance was tightened after September 11 was through the appropriation of ordinary commercial data – convenience store video tapes, telephone company customer logs, car rental records, credit card purchase data, Internet ticket sales, and email messages stored by service*

---

66 See product fact sheet at http://www.sas.com/technologies/analytics/datamining/miner/

67 See SAS case study at http://www.sas.com/success/floridadoc.html

providers. All this transactional data may be trawled – using permissive 'routine use' clauses or special powers to over-ride privacy or data protection law in pursuit of after-the-event investigations.[68]

Financial institutions that provide credit and debit cards receive detailed records of the location, the time and the amount customers have spent on different items. Retailers are increasingly willing to accept cards for small purchases, and many consumers seem to value the convenience of avoiding the need for cash, making available even more purchase information to card providers. The large global credit card associations acquire data on an enormous volume of purchases every year:

MasterCard operates in 210 countries, handles an average of $6 billion transfers a day, and did $1.25 trillion worth of transactions in 2002. So how does a company that has 320 TB of data build its storage infrastructure…? On the new network, MasterCard's data warehouse allows it to store four years of transactional data and make it available to customers so they can use the information. Now they can perform data mining, even on a global scale, with the ability to analyze worldwide trends.[69]

Many companies also provide detailed information on their customers and employees to credit reference agencies such as Experian:

It holds detailed records on 40 million individuals in Britain and last year carried out 80 million checks on us on behalf of 300 other companies, as well as the police and social security officials…

Experian knows who you are, where you live, and where you used to live. It knows who you bank with, who you have credit cards with and whether you have kept up the payments. It knows if you have any court judgments against you, past bankruptcies or even voluntary arrangements with creditors. It will even tell other companies if you have failed to disclose any "detrimental data".[70]

The introduction to the UK of loyalty cards in the mid-Nineties and their continued popularity has led to the creation of another large new source of data on buying habits. Cards allow supermarkets in particular to build up a very detailed picture of their customers' lives, which enables highly personalised marketing. The joint Nectar card scheme launched in 2002 by Sainsbury's, Barclaycard, BP and a range of other retailers had signed up almost half of the UK's 22 million households in its first five months of operation, and therefore has a very large range of databases of consumer behaviour to analyse for the benefit of its members[71].

Radio Frequency Identity (RFID) devices in loyalty cards, goods and building infrastructure could provide further information to retailers by allowing shoppers to be tracked as they move around stores. Goods that a customer had spent some time looking at or picking up could be noted to allow later targeted marketing.

The oft-cited rule of thumb that 80% of many company's profits come from 20% of their customers has provided an even more direct incentive for companies to get to know their customers better. By identifying those 20% of key consumers, companies can provide their best customers with improved customer service to increase loyalty, while also encouraging them to try out more profitable goods and services. Less

---

[68] See background on The Surveillance Project, Queen's University at http://qsilver.queensu.ca/sociology/Surveillance/narrative_report.htm

[69] Megan Loncto. Credit card company masters storage. SearchStorage.com, 30 October 2003. Available from http://searchstorage.techtarget.com/originalContent/0,289142,sid5_gci934314,00.html

[70] Patrick Collinson. This is your life. The Guardian, 7 September 2002. Available from http://www.guardian.co.uk/bigbrother/privacy/yourlife/story/0,12384,785900,00.html

[71] Rachel Shabi. The card up their sleeve. *The Guardian*, 19 July 2003. Available from http://www.guardian.co.uk/weekend/story/0,3605,999866,00.html

valuable customers can be given a standard level of service, or even encouraged to shop elsewhere.

Customer Relationship Management (CRM) software is a growing market that could in time also be mirrored in cooperative police systems. It allows companies to capture every detail of their interactions with each customer, and build up a profile that can be used to determine how to most profitably deal with them. Online stores can use their detailed records on browsing, purchase behaviour and previous searches to market related products to customers when they return to the web site.

In particular, as companies learn more about their customers' willingness to pay for products, they are able to charge prices closer to that level. Airlines have shown how profitable such price discrimination can be, charging business travellers a large multiple of the price at which the same seat would have been available a month earlier to a bargain-hunting tourist. Large databases may enable this type of pricing model to be extended to many other markets[72].

All of these factors encourage companies to store large amounts of data on their customers. But it is not clear how much of this data would prove useful for large-scale data mining by law enforcement, as has been proposed in the US under *Total Information Awareness*. Much is information of a quality quite adequate for marketing, where a mistargeted piece of direct mail advertising only costs the company the price of delivery of a letter. But if these databases were searched for "suspicious" purchasing patterns, shoppers should perhaps be more careful about making purchases for friends and family or buying unusual items that will end up in their customer records.

Open source intelligence

Part of the growth in the amount of information available on the World Wide Web described earlier has been in various forms of personal data. Some of this is explicitly published by an individual. Some is made available by other interested individuals or organisations.

Many Web users maintain home pages that give information about themselves, their friends and families. A newer trend is for users to publish weblogs or blogs, similar to an online diary, where the author describes their recent experiences, interactions and thoughts.

Online discussion groups are older but equally popular. Participants discuss a huge range of subjects, which are sometimes potentially sensitive such as health-related topics. These groups often have a Web archive where messages in the discussion can be read later by any Web user.

Finally, information about individuals is contained on more traditional media Web sites – newspapers, television and radio stations – community information boards and online government information sources such as court records.

These fragments of personal information scattered around the Web can be collated using a search tool such as Google, and combined into a more detailed profile. Discussion group archives in particular may reveal the opinions and thoughts of an individual that could have changed in the intervening period.

Communications surveillance

Information from and about personal communications is obtained by police in the UK under two distinct categories. Interception of the *content* of communications

---

[72] Privacy, economics, and price discrimination on the Internet, A. M. Odlyzko. *ICEC2003: Fifth International Conference on Electronic Commerce*, N. Sadeh, ed., ACM, 2003, pp. 355-366. Available from http://www.dtc.umn.edu/~odlyzko/doc/privacy.economics.pdf

(what is actually said in a telephone call or in the body of an e-mail) is carried out with the authorisation of a Secretary of State. Such "lawful intercepts" can now make use of features designed into communications equipment to make interception relatively easy from a technology perspective. The government has powers to instruct phone companies and Internet Service Providers to install equipment that provides these features.

Information *about* communications (who a given user has been calling or e-mailing, which web sites they have visited and where their mobile phone has been operating) is separately classified as *communications data*. This information is accessed by police through the authorisation of a senior police officer (Superintendent or above[73]). The government is able to mandate the length of time that telecommunications companies store different types of communications data. Under the current voluntary scheme this is 4 days for Web sites visited, six months for e-mail details and twelve months for phone contacts[74]. The pending mandatory arrangements may differ.

This section provides detail concerning the trends in technology and law that affect lawful intercept and access to communications data.

Lawful intercept

During the 90's Internet boom, a vast amount of new communications equipment was put in place as telecommunications companies upgraded their networks and provided new services based on the Internet Protocol.

In the first phase of this transition to digital networks, the US Congress was persuaded that telecommunications companies should be paid $500m to provide "lawful intercept" wiretapping services on their networks. This allows the content of telephone calls to be supplied as they happen to law enforcement agencies, pursuant to lawful authority. Under the Communications Assistance to Law Enforcement Act (CALEA) of 1994, telephone companies and their equipment suppliers and manufacturers face fines of up to $10,000 per day if a court order to provide this functionality is not met. As many of these manufacturers are large global companies[75], the wiretapping services are becoming available in communications networks around the world.

Such legal regimes have encouraged the development of computing standards for lawful intercept. Groups such as the Organization for the Advancement of Structured Information Standards[76] and the European Telecommunications Standards Institute[77] are developing standard mechanisms by which communications equipment can provide copies of the voice, video or other types of data travelling to or from a specific user, in close to real time, to law enforcement agencies. The only major standards body to so far to refuse law enforcement requests to include lawful intercept capabilities in its protocols is the Internet Engineering Task Force, which decided after a heated debate that such capabilities should not be featured in global standards[78]. However, the underlying telecommunications infrastructure that carries Internet traffic is still becoming ever-more convenient to intercept.

Laws similar to CALEA have been passed in other countries including the UK. The Regulation of Investigatory Powers Act 2000 s.12 allows the government to impose requirements on public telecommunications networks:

---

73 Regulation of Investigatory Powers (Communications Data) Order 2003

74 Latest version of the Code is available at http://www.legislation.hmso.gov.uk/si/si2003/draft/5b.pdf

75 e.g. see the description of top-selling Cisco Systems' Internet router functionality at http://news.com.com/2010-1071-997528.html

76 See http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=legalxml-intercept

77 See http://www.etsi.org/

78 IETF Policy on Wiretapping. IETF Request for Comments 2804. Available from http://www.ietf.org/rfc/rfc2804.txt

for the purpose of securing that it is and remains practicable for requirements to provide assistance in relation to interception warrants to be imposed and complied with.

The Regulation of Investigatory Powers (Maintenance of Interception Capability) Order 2002 sets out more detail on what these obligations may comprise. Public telecommunications service providers may be obliged to do any or all of the following:

- *To provide a mechanism for implementing interceptions within one working day of the service provider being informed that the interception has been appropriately authorised.*
- *To ensure the interception, in their entirety, of all communications and related communications data authorised by the interception warrant and to ensure their simultaneous (i.e. in near real time) transmission to a hand-over point within the service provider's network as agreed with the person on whose application the interception warrant was issued.*
- *To ensure that the intercepted communication and the related communications data will be transmitted so that they can be unambiguously correlated.*
- *To ensure that the hand-over interface complies with any requirements communicated by the Secretary of State to the service provider, which, where practicable and appropriate, will be in line with agreed industry standards (such as those of the European Telecommunications Standards Institute).*
- *To ensure filtering to provide only the traffic data associated with the warranted telecommunications identifier, where reasonable.*
- *To ensure that the person on whose application the interception warrant was issued is able to remove any electronic protection applied by the service provider to the intercepted communication and the related communications data.*
- *To enable the simultaneous interception of the communications of up to 1 in 10,000 of the persons to whom the service provider provides the public telecommunications service, provided that those persons number more than 10,000.*
- *To ensure that the reliability of the interception capability is at least equal to the reliability of the public telecommunications service carrying the communication which is being intercepted.*
- *To ensure that the intercept capability may be audited so that it is possible to confirm that the intercepted communications and related communications data are from, or intended for the interception subject, or originate from or are intended for transmission to, the premises named in the interception warrant.*
- *To comply with the obligations set out in paragraphs 5 to 13 above in such a manner that the chance of the interception subject or other unauthorised persons becoming aware of any interception is minimised.*

However, even a network that implements all of these requirements will not be able to intercept all of the communications of their customers. If customers encrypt their data (see later section) the messages will only be readable at the point of destination. It will also be difficult to identify users of relatively anonymous Internet cafes and free e-mail Web sites with the intention to intercept their communications.

Communications data retention and access

Law enforcement access to information *about* the details of communications is known as *communications data access*. This type of data covers telephone numbers called, e-mail contacts, web sites visited and even the location of mobile telephones.

Law enforcement access to this category of data (taken separately from the content of phone calls) became easier with the development of digital telephone exchanges and their ability to perform itemised billing. Access to this billing data provided a relatively easy way for law enforcement agencies to discover with whom a given suspect had been communicating. British Telecom even provided police with a direct computer link to its billing databases. No external authorisation is required for law enforcement agencies to access this category of data.

This use of call records became much more pervasive with the creation of *friendship tree* analysis software that can take very large lists of telephone calls made between many different numbers and work out patterns such as which sets of numbers call each other most regularly, and hence whose owners are likely to have some kind of relationship (see the later section on information analysis tools). These techniques encourage investigators to acquire large volumes of call records in an attempt to identify numbers of interest.

With the popularisation of the Internet, data about many new types of communications – e-mails, web surfing, instant messaging – became available. Location data generated by the radio connection between mobile telephones and the nearest "base station" through which they connect to the phone network is also available to network operators:

> *The accuracy of location data varies by location area as well as the technology used by networks. Location ... in cities, where there are relatively small cells, could be accurate to within 100m or so, although typically accuracy is between 500m—2km. In sparse areas of the countryside it may only be accurate to 15km.*
>
> *Networks can request a more detailed "measurement report" from phones which includes timing information allowing location to about 270m.*
>
> *Even more detail can be obtained by triangulating data on other base stations in range of a phone. This capability is required in the US by Enhanced-911 government rules on emergency calls, and is included in Phase 2 of the GSM specification (which is the basis for mobile networks in most countries around the world outside the US).*
>
> *Third-generation (3G) networks, which are already being rolled out in several European countries, can be much more accurate – down to 10m. Several countries (such as the US) have mandated that phone networks achieve this level of accuracy during the next few years so that callers to emergency services can be located if their location is unknown, or if the call is lost halfway through.* [79]

This rich new set of data – particularly all of the information that a Web user is accessing and the location of a mobile phone user – might be considered closer in its potential for privacy invasion to the content of a communication than to an itemised phone bill. This was indeed the view given to Parliament by the previous UK Information Commissioner[80].

---

[79] Ian Brown. The danger to journalists from new security technologies. In *Spreading the word on the Internet: reflections on freedom of the media and the Internet*, Vienna: Organisation for Security and Co-operation in Europe, pp.187-196, October 2003.

[80] Response of the Data Protection Commissioner to the Government's Regulation of Investigatory Powers Bill: A briefing for Parliamentarians. March 2000. Available from

However, the data have instead been grouped with phone records for the purposes of regulating access. Communications data are available to the police in the UK under a much lower standard of authorisation than is access to the content of communications. Until recently, police requested the data from *Communications Service Providers* (phone companies and Internet Service Providers) and relied on s.29 of the Data Protection Act 1998 to exempt the disclosure from data protection requirements. In January 2004 a new regime was brought into force under the *Regulation of Investigatory Powers Act 2000* that allows the police to require the disclosure of communications data using a notice signed by a senior officer. This procedure permits the police themselves to judge whether a specific disclosure is proportionate, with the marginal possibility of a subsequent check by the Interception Commissioner.

Mobile phone companies have already complained that they are being overwhelmed by police requests for data regarding calls[81]. The Home Office estimates that around half a million requests for communications data are made every year, with the All Party parliamentary Internet Group putting the figure closer to one million[82].

It is therefore not difficult to foresee the development of more automated retrieval systems between the police and Communications Service Providers (CSP's), as both parties would benefit: the police in faster access to data, and the CSPs in reduced costs once the retrieval system is in place. These cost savings also benefit the police, who are required to pay the costs incurred by CSPs in retrieving data. There is therefore a strong economic incentive to encourage the simplification of police access to communications data. Full automation does of course remove the extra check that was previously in place whereby a CSP staff member scrutinised and answered requests for data.

One UK private sector organisation[83] has already been set up to check and then forward requests for communications data from government agencies to CSP's, however the data is returned directly from the CSP to the requesting agency.

The final stage in the simplification of access would be for a government agency to hold copies of the communications data generated by all of the UK's phone companies and ISPs. The Association of Chief Police Officers, Customs and Excise and the UK intelligence agencies proposed such a *data warehouse* in 2000, explaining that it would "facilitate an immediate and simultaneous search across all the data generated by UK CSPs"[84] Data would be stored for up to seven years.

This proposal was rejected by the Home Office, which instead pushed ahead with *data retention* plans in the *Anti-Terrorism, Crime and Security Act 2001*. This allows the government to order CSPs to store communications data for a specified period by way of secondary legislation should a voluntary agreement fail to achieve that objective. These powers were renewed in November 2003 but have not yet been used.

The UK could still see the development of communications data warehouses in the private sector if CSP's decide to outsource the provision of that data to law enforcement. *Verisign*, for example, provide a *NetDiscovery* programme in the US that:

---

http://www.dataprotection.gov.uk/dpr/dpdoc.nsf/ed1e7ff5aa6def308025663600 45bf4d/3fddbd098455c3fe802568d90049ac04?OpenDocument

81 Phone firms 'flooded' by crime checks. *BBC News Online*, 20 December 2002. Available from http://news.bbc.co.uk/2/low/uk_news/2592707.stm

82 Communications Data: Report of an Inquiry by the All Party Internet Group, January 2003. Available from http://www.apig.org.uk/APIGreport.pdf

83 See http://www.singlepoint-dataservices.co.uk/home.html

84 Roger Gaspar. Looking to the future: clarity on communications data retention law. Submission to the Home Office on behalf of the Association of Chief Police Officers and others, 21 August 2000. Available from http://cryptome.org/ncis-carnivore.htm

> *Provides carriers with a complete solution to meet the legal, technical, and operational requirements of the Communications Assistance for Law Enforcement Act (CALEA) as set by the FCC. NetDiscovery includes provisioning, access, and delivery of call information from carriers to law enforcement agencies (LEAs).*[85]

One driver for such a service in the UK may be the facility to store communications data in a manner that complies with data retention rules once there was no remaining business purpose for it to be kept by the Communications Service Provider.

All of these trends – the provision of greater amounts of information about communications, at lower cost, via centralised providers – will encourage police use of such data. The availability of ever-more sophisticated friendship network analysis tools will also create an incentive to gather increasing amounts of data on the activities of suspects' contacts in the hope that greater acquisition of data reserves will improve the quality of analysis.

Authorisation and oversight

Interception warrants in the UK are authorised by a Secretary of State. The results of intercepts cannot be adduced as evidence in court. While there is an ongoing debate in the government about changing this position, intelligence agencies do not wish the success (or otherwise) of their interception operations to become public knowledge by way of court cases[86].

In a letter dated 16 August 2002 in response to an Open Government request by Privacy International, the Home Secretary's Private Secretary, Jonathan Sedgwick, said that the Home Secretary receives an "oral" presentation of warrant applications "three or four" times a week, prepared and recommended by Home Office officials. In the Home Secretary's absence, any of the fourteen Secretaries of State can authorise interception warrants, including those with responsibilities for culture, media and sport, and education. All that is required to authorise warrants is a "briefing" of responsibilities under the relevant legislation.[87]

Oversight of access to communications data and of the regime of communications interception is handled by the *Interception of Communications Commissioner*, The Rt. Hon. Sir Swinton Thomas. The 2001 annual report of the Interception Commissioner[88] found over 40 errors by police and intelligence services when conducting wiretaps.

Concern has been expressed that the planned oversight arrangements by the Interception Commissioner will be inadequate. In a briefing to the House of Lords, FIPR noted:

> *We do not believe that one centralised office (of the Interception Commissioner) can provide proper oversight of more than one million requests per year. Even when properly resourced, the office will only be able to examine a tiny fraction of the total requests made. A central record of requests is not planned; the Interception Commissioner will need to visit hundreds of bodies around the country annually under current government proposals.*[89]

---

85 See http://www.verisign.com/telecom/products/network/netDiscovery.html

86 David Leigh and Richard Norton-Taylor. MI6 fights to block phone tap evidence. *The Guardian*, 14 October 2003. Available from http://www.guardian.co.uk/crime/article/0,2763,1062530,00.html

87 Correspondence at http://www.privacyinternational.org/countries/uk/surveillance/interceptioncomm.html

88 See http://www.privacyinternational.org/countries/uk/surveillance/inter-comm-report-2001.pdf

89 Foundation for Information Policy Research briefing. Available from http://www.fipr.org/030818ripa.html

Speaking in debate on Orders relating to the Regulation of Investigatory Powers Act, the Earl of Northesk remarked:

> *There are considerable problems too with "monitoring, scrutiny and accountability" of both the retention and access regimes. I acknowledge that this is probably not relevant per se to the orders. Nevertheless it is important to understand the context in which the respective regimes will operate. It has been estimated that the Office of the Interception Commissioner will have oversight of more than a million surveillance requests per year, although I suspect that the Home Office considers that that figure is rather overstated. Whatever the true figure, even when properly resourced, it is unlikely that the office will be able to examine more than a fraction of the total requests made. It should be noted too that the Information Commissioner has already reported "significant" and "unacceptably high" numbers of errors in RIPA Part 1 Chapter I interception warrants.* [90]

Lord Northesk also echoed an ongoing concern about the right of redress regarding both Interception and Communications Data Access:

> *The Home Office, and, indeed, the noble and learned Lord the Attorney-General, may wish to parade the success rate of the interception of communications and investigatory powers tribunals as testimony of the robustness of this element of the oversight regime. However, for the convenience of the noble and learned Lord I confirm that of the 470 cases considered by them between 1996 and 2003, none was adjudicated in favour of the complainant.* [91]

Identification technologies

DNA databases

The UK's National DNA Database (NDNAD) was established in 1995 under the custodianship of the Forensic Science Service (FSS) on behalf of the Association of Chief Police Officers (ACPO).[92] Its' original primary goal was to assist the detection of serious crime suspects, relating in particular to such crimes as sexual assault and burglary where the chance of discovering forensic evidence on crime scenes or victims is greatest.

The legal infrastructure to support the collection of DNA samples had by then already been established. The *Criminal Justice and Public Order Act 1994* included powers to take non-intimate samples from individuals charged, reported, cautioned or convicted for recordable offences from 10 April 1995 onward, or who were convicted of sex, violence or burglary offences before that date if they were still serving a prison sentence at the time the sample was taken. The *Criminal Justice and Police Act 2001* allows the indefinite retention of DNA samples from all criminal suspects. The Act also permitted police to take samples at the point of arrest, rather than at the point of charge, further expanding the database. Powers were given to the police to keep sample details on their own systems for ease of matching. From the late 1990's a small number of area forces such as Lothian and Borders pioneered the practice of taking DNA samples from anyone charged with any recordable offence.[93]

---

90 Hansard, 13 November, 2003. Available from http://www.publications.parliament.uk/pa/ld199900/ldhansrd/pdvn/lds03/text/31113-04.htm#31113-04_spnew2

91 Ibid.

92 Factsheet about the National DNA Database, Forensic Science Service. Available from http://www.forensic.gov.uk/forensic/foi/foi_docs/NDNADFactSheet.pdf

93 The Police and Criminal Evidence Act (Sections 62, 63 and 65), as amended by the Criminal Justice and Public Order Act 1994 and Section 82 of the Criminal Justice and Police

By 2003 the NDNAD contained more than two million samples and profiles relating to specific individuals. The Home Office hopes by the end of 2004 to have captured profiles of the whole active criminal population (currently projected to be 2.6 million offenders). 2003/2004 funding for this work is £61m.[94] There are currently 180,000 DNA profiles from samples at crime scenes on the database. 57,000 samples were loaded in 2002/03.[95]

The Home Office claims there is a 40% chance that a crime scene sample will be matched immediately with an individual's profile on the database. In a promotional publication the Department notes that in a typical month matches are found linking suspects to 15 murders, 31 rapes and 770 motor vehicle crimes:

> *In 2002 there were around 21,000 detections in crimes where DNA evidence was available, a 132% increase since 2000. In crimes where a DNA profile has been obtained, the rate of crimes detected increases to 37% from the overall average of 24%.*[96]

The NDNAD comprises a substantial spectrum of personal data. The following fields, derived from a subject access request, comprise a file on the national DNA database:

Name
Date of Birth
Alias 1
Alias 2
Gender
Country
Paternity Id
Ethnic Origin
Sample Barcode
Sample Type 3
Case Class Code:SA
Case reference
Recordable offences
Case Reference
Arrest Summons
Batch Reference
No in Batch
Gel Number (+Track No);
Test Type: 3

The document continues:

> *Each DNA sample is tested against a number of different DNA markers or Loci. Each test is expected to detect two values, one from each parent. Sometimes the same result will be obtained from both parents. The Amelogenin marker (Amel) is indicative of the person's gender.*[97]

The existence of a NDNAD profile is flagged on the Police National Computer, marked against the relevant name or alias entries.[98]

Act 2001, allows intimate and non-intimate samples to be taken and profile details to be retained on the national DNA Database

94 Police Science and Technology Strategy

95 Forensic Science Service. DNA: 21st century crime fighting tool, 2003. Available from http://www.homeoffice.gov.uk/docs2/dnacrimeightingtool.pdf

96 Ibid.

97 Subject Access Request form to the Forensic Science Service lodged in 2002 under the Data Protection Act. An example of this form can be found at http://www.nutteing.50megs.com/dnapr.htm

98 Authors' interview with Phillip Webb, PITO

DNA has acquired a reputation for near-infallibility. However the matching technique, the record-keeping processes and the associated forensic chain may be less precise. There have been a number of reports of "positive" matches being made in circumstances where the alleged perpetrator could not have committed the crime. One man was matched with DNA at a crime scene and yet was in prison at the time, another man was arrested for murder in a country he had never visited,[99] while another severely disabled man was offered compensation by police after a false match with a crime scene sample resulted in his wrongful arrest.[100] Senior officials responsible for police scientific development have acknowledged that such errors pursued through the legal process could jeopardise the DNA profiling regime.[101]

A key factor determining the true reliability of DNA matching lies in the disparity between the theoretical accuracy of the technology, and the accuracy level that is limited by the profiles established by the NDNAD. Nevertheless, the technology is touted as almost foolproof. As one peer reported in debate in the House of Lords:

> *The technology surrounding DNA evidence has advanced, so much so that in a recent United States case it was said that the odds against someone else having committed the crime were 73 trillion to one; namely, more human beings than have existed since Creation.*[102]

Another popular figure has been cited by former Home Office Minister Charles Clarke:

> *The more advanced SGM plus technique was introduced by the FSS in September 1999. A statistical assessment, to be published in the International Journal of Legal Medicine, showed that when using this process the probability of a chance match between a full DNA profile obtained from a suspect's sample and another one from a crime scene stain left by another person was less than one in a billion.*[103]

Despite indications that the technique of DNA matching is less precise than folklore would suggest, there appears to be considerable support within the law enforcement community to extend the DNA sampling regime even further, possibly to the extent of creating a universal collection system.[104] While such a proposal has not found immediate political support there has been a considerable expansion in the number of people who have been DNA tested. Large-scale research projects such as BioBank have promoted anonymity as a core component of their work[105] but 'anonymous'

---

99 Chris Johnson. Cleared murder accused victim of DNA blunder. The Liverpool Echo, Mar 10 2003. Available from http://icliverpool.icnetwork.co.uk/0100news/0100regionalnews/page.cfm?objectid=12718961&method=full&siteid=50061

100 Disabled man turns down payout offer. This is Wiltshire, 15 December 2000. Available from http://cjpa.freeservers.com/easton.htm

101 Authors' interview with Phillip Webb, PITO, February 2004

102 Lord Williams of Mostyn, Hansard, 8 May 2001 Available from http://www.publications.parliament.uk/cgi-bin/ukparl_hl?DB=ukparl&STEMMER=en&WORDS=nation+dna+databas+&COLOUR=Red&STYLE=s&URL=/pa/ld200001/ldhansrd/vo010508/text/10508-16.htm#10508-16_spnew1

103 House of Commons, 17 November 2000. Available from http://www.publications.parliament.uk/cgi-bin/ukparl_hl?DB=ukparl&STEMMER=en&WORDS=reliabl+dna+evid+&COLOUR=Red&STYLE=s&URL=/pa/cm199900/cmhansrd/vo001117/text/01117w05.htm#01117w05.html_spnew7

104 "Have the police hijacked our DNA?"; Editorial, *The Lancet*, September 2003. Available from http://www.scienceblog.com/community/older/2003/F/20033662.html. See also Call for National DNA Database. *BBC News Online*. May 5 1998. Available from http://news.bbc.co.uk/1/hi/uk/87948.stm. Also Simon Jeffrey. Police seek DNA records of everyone. *The Guardian*, September 8, 2003. Available from http://www.guardian.co.uk/crime/article/0,2763,1037584,00.html

105 Steve Connor. DNA database pledges to defend confidentiality. *The Independent*, 25 August 2003. Available from http://news.independent.co.uk/uk/crime/story.jsp?story=436925

medical data has been used in prosecution, resulting in concern amongst the research community that public confidence may be eroded in such data stores.[106]

The analysis of increasingly small samples of DNA is yielding greater information. The Science and Technology Strategy states that identifying individual characteristics from DNA is a short to medium term goal. A substantial amount of research within the UK and internationally is exploring the potential to increase the information that can be derived from DNA samples. The House of Lords Standing Committee on Science and Technology reported the possibility that:

> *...genetic technologies would assist the determination of distinctive traits (such as hair colour, eye colour, ethnicity, weight and height) which might ultimately contribute to the identification of individuals. (QQ 129-131).* [107]

As reported in the Science and Technology Strategy, work is being undertaken to find methods of producing "lab on a chip" technology that would permit roadside analysis of DNA samples linked directly to the NDNAD. Research is also being conducted on the development of a hand-held DNA testing kit to be carried and operated by police officers during regular patrols. The device would be connected to the national NDNAD via the Airwave system.[108]

ID cards and biometrics

The current Home Office proposal[109] for a national ID card carries some important implications for the functioning of law enforcement agencies and for the privacy rights of individuals.

The relationship between a card system and the police has so far centred on the issue of the right of police to demand the card and the responsibility of the citizen to carry it. The Home Secretary has given assurances in Parliament that even when the card becomes compulsory people will not be required to carry it at all times. This was reinforced at the first ID card hearing of the Home Affairs Committee when a Home Office official explained:

> *The desire of the Home Office is to have a compulsory scheme. Certainly as now, if the police stop you for speeding, they can ask to see your driving licence, but there is no an expectation that you will always have it with you. We would expect exactly the same situation, the same culture. Ministers have been very clear, right from the outset, that they do not want a compulsory to carry scheme. For that very reason we do not want to move to a "Big Brother State" where you are having to produce a card at all times.*[110]

Such assurances, as evidenced by the recent establishment of higher education top-up fees, may only be given for the life of the current Parliament, and cannot be binding on future administrations. They may well be subject to revision. Countries such as the Netherlands have recently created a legal compulsion to carry identity cards at all times.[111] In reality, it is likely most of the UK public will carry the card at

---

106 Steve Connor. Police access to medical data 'a threat to research'. *The Independent*, 16 July 2001. Available from http://millennium-debate.org/ind16july014.htm

107 House of Lords Select Committee on Science & Technology; 4th Report, 2001. Available from http://www.publications.parliament.uk/pa/ld200001/ldselect/ldsctech/57/5706.htm#n29

108 David Cracknell. Roadside DNA tests planned. *The Daily Telegraph*, London, 10 December 2000. Available from http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2000/12/10/nkit10.xml

109 Home Office. Identity Cards: the Next Steps. Cm 6020, November 2003. Available from http://www.homeoffice.gov.uk/docs2/identity_cards_nextsteps_031111.pdf

110 Evidence of NicolaRoche to the Home Affairs Committee. 11th December 2003 http://www.publications.parliament.uk/pa/cm200304/cmselect/cmhaff/uc130-i/uc13002.htm

111 The 'Wet op de uitgebreide identificatieplicht' law gives a wide range of government and law enforcement officials the power to demand identification in the course of their duties. A penalty of €2,250 (US$2,500) will apply to anyone who does not comply. Refusal will

all times to avoid the inconvenience of having to travel the following day to a police station should they be requested to produce it.

A 1994 Privacy International survey of ID cards found claims of police abuse by way of the cards in virtually all countries surveyed.[112] Most involved people being arbitrarily detained after failure to produce their card. Others involved beatings of juveniles or minorities. There were even instances of wholesale discrimination on the basis of data set out on the cards.

While it is true that cards containing non-sensitive data are less likely to be used against the individual, cards are often alleged to be the vehicle for discriminatory practices. Police who are given powers to demand ID invariably have consequent powers to detain people who do not have the card, or who cannot prove their identity. Even in such advanced countries as Germany, the power to hold such people for up to 24 hours is enshrined in law. The question of who is targeted for ID checks is left largely to the discretion of police.[113]

Such concerns have been echoed in the UK by *Liberty*, the *Commission for Racial Equality*, the *Law Society* and the *1990 Trust*.

However, the issue of police power to demand on-the-spot disclosure of the card is only one small aspect of the proposal. The current Canadian Parliamentary *Committee on Citizenship and Immigration* study on a national ID card proposal has noted considerable concern amongst witnesses about police "stop and demand" powers, but the Committee also signalled a range of equally significant concerns.[114] If the national ID number is to be used as a general administrative base for the sharing of data, and if a biometric used as a key means of authentication, then a range of issues are raised concerning interactions between the police and the public. As Privacy International noted in its submission to the Canadian Inquiry:

> *The modern ID card is not merely a simple piece of plastic. It is the visible component of a highly complex web of interactive technology that fuses the most intimate characteristics of the individual, with the machinery of state. It is also the means by which legal and administrative powers of government can – in theory - be both streamlined and amplified. Almost every national ID card system introduced in the last fifteen years has contained three components that have the potential to devastate personal freedom and privacy. To begin, each citizen may be obliged to surrender a fingerprint or retina print to a national database. This information is combined with other personal data such as race, age and residential status. A photograph completes the dossier. Then, in order to give the card the necessary legal gravity, its' introduction must be accompanied by a substantial increase in police power. Authorities will, after all, want to demand the card in a wide range of circumstances, and people must be compelled to comply. The most significant, yet most subtle, element is that the card and its numbering system then form the administrative basis for a linkage of information between all government departments. The number is ultimately the most powerful element of the system.*

Police organisations broadly support the UK proposal, if for no other reason that its' potential to help streamline the management of police data. Both the Police National Computer (PNC) and the different police intelligence systems sort data according to

---

constitute a criminal offence. The law institutes both the *toonplicht* requirement (obligation to disclose ID) and the *draagplicht* requirement (obligation to carry ID).

112 Report available at: http://www.privacyinternational.org/issues/idcard/idcard_faq.html#9

113 Ibid.

114 Report available at http://www.parl.gc.ca/InfocomDoc/Documents/37/2/parlbus/commbus/house/reports/cimmrp06/cimmrp06-e.pdf

case and file rather than by unique person. A national ID number, they believe, would not only allow an administrative base for linking and sharing law enforcement data, but would also enhance capabilities to match data across the private and public sector.

However, oral evidence so far given to the Home Affairs Committee has indicated that many practical questions remain unanswered. Patronage of the idea of an ID card has been pursued with little quantifiable evidence of the claims made by its proponents. The presumption, for example, that a national card can improve law enforcement techniques, reduce illegal immigration, diminish fraud, assist national security or improve administrative efficiency has so far been largely instinctive – a view reinforced by the Canadian Parliamentary Inquiry Interim Report.[115] There is little, if any, evidence that a card system can achieve these goals. The proposed national biometrics element has been subjected to even lighter scrutiny.

The biometrics system proposed for the UK card is likely to use one of three technologies: face recognition, fingerprints or iris scans. Face recognition systems attempt to match pictures of individuals, usually from CCTV cameras, against those stored in a database. Fingerprint scanners match one or more prints taken electronically against reference prints in a database. Iris scans do the same using specific characteristics of the eye.

One objective of the Home Office scheme is to prevent individuals registering with multiple identities. This means that central databases of these biometric records will need to be kept for comparison with new applications for cards. It is unlikely that these databases will be used directly by the police in the next five years, not least because of potential incompatibilities between systems. However, this would remain an option for the future.

PITO is also investigating biometric identifiers. Their forward plan states that: "*Development and wider deployment of Livescan fingerprint scanning systems will be undertaken. Biometrics, including face and voice recognition, will be investigated.*" PITO is also working to "*Establish the police requirement and business case for a facial images national database, drawing on the Home Office Police Science and Technology Strategy.*"

US security experts Peter Neumann and Laurie Weinstein have observed:

> *These supposedly unique IDs are often forged. Rings of phoney ID creators abound, for purposes including both crime and terrorism. Every attempt thus far at hardening ID cards against forgery has been compromised. Furthermore, insider abuse is a particular risk in any ID infrastructure. The belief that "smart" NID cards could provide irrefutable biometric matches without false positives and negatives is fallacious. Also, such systems will still be cracked, and the criminals and terrorists we're most concerned about will find ways to exploit them, using the false sense of security that the cards provide to their own advantage – making us actually less secure as a result.*[116]

Again citing Privacy International's submission to the Canadian Parliament:

> *When such schemes are introduced in the current climate, three outcomes are inevitable. First, a high security ID card will become an internal passport, demanded in limitless situations. Don't leave home without it. Second, millions of people will be severely inconvenienced each year through lost, stolen or damaged cards or – more potentially devastating - through failure of the card's computer systems or the biometric reading machinery. Finally, as*

---

115 Ibid.

116 Peter Neumann and Lauren Weinstein. Risks of National Identity cards. *Communications of the ACM* 44, 12, December 2001. Available from http://www.csl.sri.com/users/neumann/insiderisks.html

> *research by Privacy International has shown, the cards will inevitably be abused by officials who will use them as a mechanism for prejudice, discrimination or harassment. This latter point was addressed by the UK High Court in 1954 when it outlawed the wartime ID card.*

British finance group Nationwide last year dropped plans to introduce fingerprints and iris scanning as a replacement for Personal Identification Numbers due to high costs and limited benefits[117].

Identity Theft

At first sight, it appears logical to argue that a high integrity identity system will help combat identity theft. There is, however, a substantial body of evidence to demonstrate that the establishment of centralised identity can increase the incidence of identity theft.

The clearest example of this relationship exists in the United States, where the Social Security Number has become an identity hub and a central reference point to index and link identity. Obtaining a person's SSN provides a single interface with that person's dealings with a vast number of private and public bodies. Hence the level of identity theft in the US is disproportionately high.

This situation applies equally in Australia, where the introduction of a Tax File Number has also increased the incidence of identity theft beyond the levels experienced in the UK and other countries that lack such a central numbering system.

The key element that supports identity theft is the widespread availability of a central number, linked to a range of personal information. Consumer groups in the US have recently criticised the Senate Banking Committee for failing to take action to reverse this trend. The Consumers' Union argues that identity theft will continue to rise until the relationship between the SSN and the storage of personal details in the finance sector can be reduced.[118]

Both police groups and the Home Office have supported the concept of a biometric ID card as a means of fighting identity theft. However, there are substantial security threats that arise from a biometric based identity system that may lead to identity theft becoming a problem of even graver proportions. Computer security expert Bruce Schneier warns:

> *Biometrics also don't handle failure well. Imagine that Alice is using her thumbprint as a biometric, and someone steals the digital file. Now what? This isn't a digital certificate, where some trusted third party can issue her another one. This is her thumb. She has only two. Once someone steals your biometric, it remains stolen for life; there's no getting back to a secure situation.*[119]

Electronic visual surveillance

The murder of James Bulger in 1993 was a pivotal moment in the evolution of Closed Circuit Television (CCTV). The UK population had watched, horrified and mesmerised, as the grainy images from a shopping arcade camera showed the toddler being led to his death by two ten year-old boys. The experience only confirmed what many had already suspected: video surveillance is good for crime control, and society needs more of it.

---

117 Andy McCue. Nationwide ditches iris and fingerprint biometrics. *Silicon.com*, September 23 2003. Available from http://www.silicon.com/news/500013/1/6129.html

118 See Consumers' Union statement at http://www.consumersunion.org/pub/core_financial_services/000407.html

119 Bruce Schneier. Biometrics: Uses and abuses. *Communications of the ACM*, No 42, 8, August 1999. Available from http://www.csl.sri.com/users/neumann/insiderisks.html

CCTV had already been in general use for more than ten years, but the Bulger murder served as a trigger to, in effect, personalise the technology. Prime Minister John Major told the 1994 Conservative Party conference that his government was committed to CCTV, and would provide funding to expand the technology. One initiative adopted was to offer specific funding to support local CCTV projects. The Home Secretary first announced the initiative on 18 October 1994.

The House of Lords Report on *Digital Images as Evidence* reported evidence that:

> *(B)etween £150 million and £300 million is spent each year on surveillance equipment in the United Kingdom, and the Home Office has assisted in funding around 550 CCTV schemes over three 'challenge' competitions: distributing more than £37 million since 1995 (p 131). Individual schemes, for example the Chelmsford town centre system, which cost £0.5 million to set up and costs £160,000 per annum to run (The Chief Constable of Essex, Mr Burrow Q 407), represent substantial investment for a local authority. Many of our witnesses expect this scale of commitment to rise in the future.*[120]

By 1996 the Home Office estimated that 95 per cent of towns and cities had either adopted CCTV, or were planning to adopt it, to cover public areas, housing estates, car parks and public facilities. Growth in the market was then estimated at 20 to 25 per cent annually[121] and apparently increased somewhat in the late 1990's. At this level of growth the visual surveillance market in 2004 is almost ten times greater per year than in 1996.

Between 1996 and 1998 around 75 per cent of the Home Office Crime Prevention budget was spent on CCTV,[122] even though a comprehensive review has concluded that the technology will generally only produce a reduction in crime of around five per cent.[123]

CCTV has been widely deployed for a range of security, perimeter control, city management and law enforcement purposes, to the point where it has become a key plank in nearly all low level crime control, security and crime prevention policies. Its promises are promoted by government, police and media as a primary solution for urban dysfunction. Proponents of CCTV claim that the technology has been as important to the evolution of law enforcement as police radio or fingerprinting.[124]

The increasing use of CCTV has created a number of complex privacy threats. Cameras in some areas are being integrated into the urban environment in ways similar to the integration of the electricity and water supply at the beginning of the 20th century, to the extent that the technology has been dubbed the *Fifth Utility*.[125] As camera systems converge with telecommunications networks, face recognition software and a variety of law enforcement databases, their use poses a major challenge to privacy protectors.

The technology is operated by a mixture of police, local authority and private sector organisations. It is often difficult to determine which cameras are operated by which entities, despite requirements to publicly notify such details. In October 2003 Bill

---

120 House of Lords Select Committee on Science and Technology, 5th report, 1998. Available from http://www.parliament.the-stationery-office.co.uk/pa/ld199798/ldselect/ldsctech/064v/st0506.htm#a20

121 Simon Davies. Big Brother: Britain's web of surveillance. Pan Books, London 1997

122 K. Painter. Paper presented at *Ensuring the Effectiveness of CCTV* conference, London, December 2001

123 BC Welsh and DP Farrington. Crime Prevention Effects of Closed Circuit Television: A Systematic Review, Home Office Research Study 252, August 2002. Available from http://www.crimereduction.gov.uk/cctv31.htm

124 Simon Davies. Testimony before House of Lords Select Committee appointed to consider Science and Technology. Digital images as evidence, 3 February 1998

125 S. Graham. Towards the Fifth Utility? On the Extension and Normalisation of Public CCTV. In C. Norris and G. Armstrong (Eds.) *Surveillance, CCTV and Social Control.* Ashgate Publishing : Aldershot, 1998. pp. 89-112.

Brown of the New York Surveillance Camera Players organised a team to create a map[126] of cameras in part of the Leeds city centre. He found:

> *This rather small, densely packed area is watched by a total of (at least) 153 cameras: 115 installed on the exteriors of privately owned buildings, and most likely operated by private security guards; 22 hidden within uncommonly large, black-tinted globes, and most likely operated by the police; and 16 installed atop poles, and definitely operated by the City Council.* [127]

Simon Davies, Director of Privacy International, has observed:

> *As a stand-alone mechanism, the technology in the hands of authorities is a powerful tool for surveillance. In its effect - if not its intent - CCTV is defined as a technology of control. When interfaced with other technologies, its power increases substantially. The impact on rights, liberties, privacy and public life that are created by CCTV and related technologies is profound.*[128]

The true functions of the technology are reflected in the use of CCTV systems in the United Kingdom, which is currently the leading country exploiting such systems. Since its commercial inception in the late 1980s, the limits of the technology have been constantly extended. Originally installed to deter burglary, assault and car theft, in practice most camera systems have been used to combat 'anti-social behaviour', including many such minor offences as littering, urinating in public, traffic violations, obstruction, drunkenness, “rowdy” behaviour, lawful and unlawful assembly, busking, and evading meters in town parking lots. The camera systems have also been widely used to intervene in other 'undesirable' behaviour such as underage smoking, underage drinking and a variety of public order transgressions. Other applications are constantly being discovered.

> *Over the past decade, the popular view of surveillance camera technology changed radically. Once viewed as a blunt tool of surveillance, CCTV is now seen in some countries as an integral part of the urban environment. The fact that cameras have been placed into buses, trains, lifts and even phone booths has become quite ordinary. Many people now expect to be routinely filmed from the moment they leave the front gate.*[129]

CCTV technology has been in use in one form or another for more than thirty years. Its’ evolution can be divided into three distinct stages.[130]

First generation CCTV: This initial phase of the technology (still widely in use today) is best represented by the stand-alone camera connected to a monitor. The camera, often stationed as a static security device, is primarily intended for premises security, and is frequently employed in banks, domestic premises and shops. Its functions are extremely limited, and its role is almost exclusively that of crime detection and prevention. The technology is hard-wired into the premises, and is directly connected to a monitor and (usually) a recording device. Because control over this generation of CCTV has traditionally resided with individual businesses or individuals, and the images and the technology are seldom shared, the threat to privacy and civil rights has been perceived – rightly or wrongly – to be limited.

Second generation CCTV: During the late 1980’s and 1990’s, with rising concern over crime and violence, numerous towns and cities in the UK looked to ways to increase the power and scope of CCTV technology. Military

---

126 Available from http://www.notbored.org/leeds.jpg

127 Available from http://www.notbored.org/leeds.html

128 Simon Davies. Big Brother at the Box Office. The 21st International Conference on Privacy and Personal Data Protection, Hong Kong, 1999.

129 Ibid.

130 Authors’ interview with Simon Davies; January 2004

establishments and large companies had already pioneered the concept of an inter-linked network of interactive cameras with full pan, tilt, zoom and infrared capacity that could be controlled via a remote facility. The cameras – sometimes numbering in the dozens – are usually connected by way of a local area network (LAN) to a central control facility. These systems may involve sophisticated technology. Features include night vision, computer assisted operation, and motion detection facilities. Camera systems increasingly have bullet-proof casing to deal with a under-reported problem of sabotage (most new systems are designed to ensure that cameras under attack are automatically covered by neighbouring cameras). An example of an advanced wireless CCTV system is described in the section on Bandwidth and Wireless Connectivity above. Second generation CCTV systems increasingly provide digital images.

Third generation CCTV: This stage of the technology evolution fuses digital surveillance with advanced software. Technology is being developed to detect patterns in the surveillance data such through facial recognition, crowd behaviour analysis, and scanning the area between skin surface and clothes using "passive millimetre wave technology" to search for contraband or weapons.[131] Research into these technologies is receiving substantial public funding.[132]

The third generation application of CCTV has received significant attention within law enforcement and the security community. Digital CCTV allows for more substantial archiving, comprehensive wireless networking and the potential for analysis of face, gait and even behaviour.[133] The potential for use of such systems has attracted the interest of private and public sector bodies interested in pursuing "black screen" technology that would involve less operator scrutiny with, ironically, a presumption of fewer threats of privacy invasion or discrimination.[134] Research has been by EPSRC in the UK on a prototype behaviour recognition system that has been tested in Liverpool Street and Mile End Stations.[135]

The use of the technology raises key concerns regarding the application of the Data Protection Act. Given the mounting evidence that CCTV is useful as a means of making people feel safe and deterring opportunistic crime, rather than reducing or preventing major crime, it is reasonable to ask whether the notion of proportionality should be engaged. If so, then consent might become applicable. The present limitations on consent were summarised by Newham Council's security chief Bob Lack. When questioned about his attitude to the Newham residents who reported their dislike of the cameras he replied "Well I feel sorry for them, but they don't have to use our streets and shopping centres if they don't want to".[136]

---

131 Ivan Amato. Beyond X-ray Vision: Can Big Brother see right through your clothes? Discover Vol. 23 No. 7, July 2002. Available from http://www.discover.com/july_02/feattechapter.html

132 *See* United States Defense Department's Human ID at a Distance Project http://www.darpa.mil/iao/HID.htm; Kari L. Dean. Smartcams Take Aim at Terrorists. *Wired*, June 4, 2003, http://www.wired.com/news/technology/0,1282,59092,00.html; Seth Schiesel, "Security Cameras Now Learn to React," New York Times, March 6, 2003, available at http://www.nytimes.com/2003/03/06/technology/circuits/06secu.html

133 Science & Technology Strategy p.26

134 Smart software linked to CCTV can spot dubious behaviour. *New Scientist*, 11 July, 2003 http://www.newscientist.com/news/news.jsp?id=ns99993918 Mark Henderson. CCTV to spot "odd" behaviour on the Tube. *The Times*, July 10, 2003 Available from http://www.timesonline.co.uk/newspaper/0,,173-740589,00.html

135 EPSRC Briefing: Crime Prevention and Detection Technologies, November 2002. Available from http://www.epsrc.ac.uk/ContentLiveArea/Downloads/Adobe%20Portable%20Document%20Format/EPSRC%20Briefing%20Note%20Number%20Five.pdf

136 *Counterblast*, BBC 2, January 1999.

Vehicle tracking

Automatic Number Plate Recognition

Speed cameras are an increasingly common feature of UK roads, with around 1,000 sites active at any one time. This is from a low base of 21 cameras in 1992 and 102 cameras in 1996[137]. This figure is likely to continue increasing given the hypothecation of revenue from camera fines to camera scheme running costs, which ensures that they can be self-funding.

So far these cameras are generally analogue units that need to be loaded with film and have pictures removed by their operators. But more sophisticated units take digital photographs which can then be analysed by software that will use Automatic Numberplate Recognition (ANPR) systems that can read a high percentage of the number plate details of pictured vehicles. This technology is also used around the City of London (the financial centre) to check for vehicles on watch lists entering the area, which can then be subjected to further scrutiny by police. It is also used at ports to monitor vehicles entering and leaving the country. Police hope to complete full camera scrutiny of the M25 in the near future[138], and have begun a process of establishing saturation monitoring of major roads in an attempt to make them "off limits" to criminals. Launching "Project Laser" in 2002, Home Office Minister John Denham remarked:

> *Automatic Number Plate Recognition is an invaluable tool in the campaign to make our streets safer. These pilots mark the beginning of an ambitious programme of crime reduction measures, harnessing the powers of technology to drive down crime. By denying criminals use of the road the police will be better able to enforce the law, prevent crime and detect offenders.*[139]

ANPR technology was adopted by numerous forces, initially on the basis of mobile "stings". In 2003 Lancashire police detained hundreds of vehicles using covert techniques, though the scanners were located in marked police vehicles. A number of non-traffic related arrests were made, involving theft, drug related and public order offences. Superintendent Graham Marshall, of Lancashire's Pennine Division, commented:

> *ANPR is a cost-efficient and effective policing tool that improves our ability to enforce the law, prevent crime, and detect offenders. It is a vital tool for detecting all sorts of crime and for reducing the number of stolen vehicles. It enables the effective deployment of resources based on intelligence and it can also play a vital role in reducing death and injury on Lancashire's roads by identifying unsafe vehicles and drivers without the correct documentation.*[140]

The central London Congestion Charging scheme, which came into operation on 17 February 2003, has been another large user of CCTV cameras connected to ANPR systems. There are around 700 cameras situated at 203 enforcement sites around the capital, with a further 64 mobile monitoring units[141]. Vehicles entering and leaving the congestion charging zone are photographed and have their registration number checked against a database of paid-up vehicles. The Metropolitan Police is looking at

---

137 National Safety Camera Liason. Questions and Answers, December 2003. Available from http://www.nationalsafetycameras.co.uk/nscl/q&a/q&a.html

138 Authors' interview with Chief Superintendent Kevin Robson, PITO, February 2004

139 Home Office press release, November 14, 2002

140 Road crime busters a hit. *This is Lancashire,* 30 August 2003. Available from http://www.thisislancashire.co.uk/lancashire/archive/2003/08/30/NEWSBLY2ZM.html

141 Transport for London. Congestion charging questions and answers. Available from http://www.cclondon.com/infosearch/dynamicPages/WF_Questionsanswers_w.aspx

using ANPR to attempt to track terrorist suspects entering London[142]. Other cities around the UK are investigating setting up congestion schemes using the same technology.

Outside of built-up areas, automatic number plate recognition is being used by the government's Vehicle Operator and Services Agency (VOSA), which equipped eight of its inspection teams with ANPR systems in 2003. These teams are initially targeting lorries and buses without MOT test certificates or licenses.

Once the MOT computerisation system is completed for all road vehicles during 2004, VOSA will be able to expand its automated checks to all vehicles. Given access to images from roadside CCTV systems, a constant check on vehicles travelling around the UK's roads could be maintained. These cameras are being deployed for purposes of traffic management on major roads as well as for speeding detection. In return, information on vehicle registration numbers that have been recognised can be fed back into police databases. *"The system is able to cover 4 lanes of traffic at any one time, day or night in almost any weather conditions, using infrared technology if necessary."*[143]

The Police Science and Technology Strategy includes ANPR vehicle tracking as a key capability. The Police Information Technology Organisation is investigating the deployment of a UK-wide system for a number of purposes:

> *Automatic Number Plate Recognition (ANPR) systems, linked to the Police National Computer (PNC) for immediate identification of stolen or wanted vehicles, are being widely deployed. Over the period of our plans the prospect is that we could further inhibit the free use of the roads to criminals.*

Police forces have already carried out trials of ANPR connected with the PNC, Driver and Vehicle Licensing Agency and local intelligence databases – although the Information Commissioner has expressed concern about the quality of the data in the DVLA database[144]. In one national six-hour trial on 21 May 2003, 60,000 number plates were scanned, leading to 1,000 vehicles being reported for offences and 65 arrests[145].

These techniques evolved from the ACPO *Operation Mermaid* campaigns that commenced in 1996. Police from all regions collaborate in these regular operations using their power to detain vehicles for safety checks, but then conducting PNC and other checks on the driver and the vehicle. The operations involve officials from the Department of Works and Pensions (DWP) and Customs & Excise, who invite the drivers to answer questions. The most recent Operation Mermaid took place on 19 September 2003.[146]

Electronically tagged vehicles

The Driver and Vehicle Licensing Agency consulted the public in the second half of 2003 on the question of whether vehicle number plates should be embedded with remotely readable electronic tags to increase their security[147]. These tags could be read by a nationwide system of roadside sensors, which would allow more accurate

---

142 BBC News Online. Congestion cameras to fight terrorism. 27 February 2003. Available from http://news.bbc.co.uk/1/hi/england/2805399.stm

143 See http://www.via.gov.uk/enforcement/anpr/anpr.htm

144 Comments by the Information Commissioner to the UK House of Commons Home Affairs Committee inquiry on identity cards at their oral evidence session on 4 February 2004.

145 Metropolitan Police. Your number's up! June 2003. Available from http://www.met.police.uk/job/job905/live_files/4.htm

146 Association of Chief Police Officers press release, 18 September 2003. Available from http://www.acpo.police.uk/news/2003/q3/opmermaid_sept.html

147 Driver and Vehicle Licensing Agency. Consultation on Vehicle Number Plate Security. Available from http://www.dvla.gov.uk/public/consult/vrm_security/vrm_security.htm

tracking of cars (or at least of their number plates) than visual recognition using cameras. For higher security, the tags could be embedded elsewhere in the car.

If the plans went ahead, the technology would enable the same set of law enforcement applications – checking for stolen, speeding, unlicensed or uninsured cars, or tracking those that are of interest to the police – as can be achieved by Automatic Number Plate Recognition.

In-car tracking devices

More sophisticated than either number plate recognition or electronic tags in cars are the use of tamper-resistant logging devices in vehicles. These "black boxes" store journey details such as location (derived from Global Positioning Satellite signals) along with vehicle speed and other information. They have been proposed in the UK as a means to perform congestion charging across the country without the need for a nationwide system of ANPR cameras or roadside transponder readers. The information would be periodically transmitted from the device to a central charging centre, which would calculate the owner's liability for charges based upon the journeys that the vehicle had undertaken. However, this is a politically sensitive proposal, and the government has undertaken not to launch a national scheme until at least 2010[148]. A trial scheme to test out the technology on lorries has already been delayed beyond 2006 due to technical problems in introducing a similar scheme in Germany[149].

A more immediate push towards the use of this technology is coming from insurance firms. The boxes would provide better accident-related data such as information on the way a damaged car was being driven before a crash. It would also allow the provision of new types of insurance such as a "Pay as you Drive" scheme being tested by Norwich Union[150].

Again, in-car tracking devices would enable the same set of law enforcement applications as number plate recognition and vehicle tags. Vehicle satellite tracking is included as a key capability in the Police Science and Technology Strategy.

Privacy Enhancing Technologies

Privacy Enhancing Technologies improve individuals' privacy by restricting the amount of information stored about their activities or by protecting information about them from unauthorised access. This could be in relation to Web browsing, sending sensitive e-mail messages or making payments.

This section describes four key Privacy Enhancing Technologies, and how their use has and might affect the amount of information available about the average citizen.

Information access controls

One of the Police Information Technology Organisation's key aims in its forward plan up to 2008 is the effective dissemination and exploitation of information across the police service. This will make it more important than ever that access to confidential data contained in police systems is properly controlled.

Strong access controls will be especially important in the longer term as sensitive data becomes available on portable terminals that can be used around the country in order to deliver 'superior knowledge at the point of decision' as envisioned by PITO.

---

148 Juliette Jowit. Black box in car to trap speed drivers. The Observer, 3 August 2003. Available from http://observer.guardian.co.uk/uk_news/story/0,6903,1011463,00.html

149 Ben Webster. Satellite tracking of vehicles hits delay. The Times, 29 October 2003.

150 William Kay. Norwich Union encourages drivers to fit "black box" tracker. The Independent, 15 March 2003. Available from http://money.independent.co.uk/personal_finance/insurance/story.jsp?story=387165

A vital part of these controls will be to prevent unauthorised access to data by internal users. In any system with a large number of users, there are unfortunately likely to be a small group who will be willing to compromise the confidentiality of data by providing copies to private detectives, journalists[151] or anyone else willing to pay for that information. A length inquiry by the Independent Committee Against Corruption in Australia in the early 1990's revealed that the unauthorised disclosure of private information from police and government sources had reached "epidemic and endemic proportions".[152] To prevent a similar occurrence in the UK strong audit trails of retrievals of confidential data will be needed to detect irregular access patterns, as well as providing evidence for investigation if allegations of wrongful usage are made.

PITO has made information protection a significant part of its forward planning, with the following work plan:

- *Support forces in adopting the ACPO Community Security Policy.*
- *Support the Central Customer in discharging its PNC Security Sub-Committee responsibilities.*
- *Facilitate the adoption of the Government Protective Marking Scheme (GPMS) across forces.*
- *Provide information security advice to national projects and provide accreditation of national police systems and infrastructure.*[153]

It is also working on information protection with the government's information security authority, the Communications-Electronics Security Group.

Encrypted data

Encryption is a key technology for information protection and hence for privacy. It allows data to be scrambled into a form that should prevent it from being read by anyone who eavesdrops on an encrypted communication or who gains unauthorised access to an encrypted file.

Encryption is an important privacy technology for police use, as it can be used to protect stored and transmitted personal data from unauthorised access. The Police Information Technology Organisation is aiming to complete the introduction of Airwave, its new encrypted radio communication system, across the country by 2005. This will prevent the interception of police communications using radio scanners as had previously occurred. The Police Science and Technology Strategy also identifies "secure exchange of data between forces and other agencies" as a key policing capability.

While encryption support has been a part of many communications standards for a decade or more, deployment in mass-market systems has been tardy. This has been due in part to political controversy over its use, as intelligence and law enforcement agencies have expressed concerns over its impact on their ability to intercept communications. It has also been due to complex software that often makes it easier for users to ignore encryption capability.

Encryption has yet to become an issue for police in the US, where it first might be expected to see significant use due to high Internet and personal computer

---

151 The Editor of the Sun gave evidence to the House of Commons Select Committee on Culture, Media and Sport that "We have paid the police for information in the past". 11 March 2003. Minutes are available from http://www.publications.parliament.uk/pa/cm200203/cmselect/cmcumeds/458/3031115.htm. There have also been a number of recent charges relating to the misuse of PNC information. See also Ciar Byrne. Four face court in police leak case. *The Guardian*, London. February 10, 2004.
http://media.guardian.co.uk/presspublishing/story/0,7495,1145113,00.html

152 See report on proceedings of a conference on the findings at
http://www.icac.nsw.gov.au/pub/public/pub2_8cp.pdf

153 PITO Forward Plan *ibid.* p.20

penetration. Figures on its occurrence during wiretaps are collated and made public by the Administrative Office of the US Courts. The Office's latest report found that:

> *"Encryption was reported to have been encountered in 16 wiretaps terminated in 2002 and in 18 wiretaps terminated in calendar year 2001 or earlier but reported for the first time in 2002; however, in none of these cases was encryption reported to have prevented law enforcement officials from obtaining the plain text of communications intercepted."*[154]

One approach that police have taken to unscramble encrypted data is to develop tools to surreptitiously capture the security information required from a suspect's computer. Some details of such a tool used by the Federal Bureau of Investigation were revealed in the high profile case of alleged mafia member Nicodemo Scarfo. The FBI clandestinely installed a Key Logger System on his personal computer, which recorded the passphrase that allowed the decryption of Scarfo's files.

Another approach is to use legal compulsion to demand the necessary security information directly from a person who has that knowledge. Part III of the UK Regulation of Investigatory Powers Act 2000 provides for two-year jail terms for those who refuse to provide such information. The Home Office is planning to bring forward secondary legislation later in 2004 to bring into force this section of the Act.

Communications anonymisers

One of the buzzwords of the last decade in communications networks has been "convergence" – the trend toward voice, video and data being carried over one set of communications links rather than over different application-specific wires. These links tend to use the Internet Protocol (IP) to carry data. This trend is slowly spreading to the home with the deployment of broadband connections which have enough capacity to carry Voice over IP calls and low-quality videoconferences as well as e-mail, Web pages and instant messages.

With this more flexible infrastructure comes the possibility of using *anonymisers* to limit the personal information revealed by the use of these communications mechanisms. These systems allow the concealment of the source and destination of communications from sender, receiver or both, as well as third parties who are able to eavesdrop on some portion of the network over which the communication travels.

One of the oldest research topics in the field of Privacy Enhancing Technologies is that of e-mail anonymisers[155]. Specialised e-mail servers known as "mixes" receive encrypted messages from users. The server decrypts the message to reveal another message, which will usually be encrypted to another mix server. After a short randomised delay, to prevent correlation between incoming and outgoing messages, the server sends on the message. After several such stages, the message reaches its final recipient, who knows only as much about the sender as the sender chooses to reveal in the message. Unlike normal messages, the route taken is not recorded in the message header.

Similar systems have been designed to allow anonymous Web browsing. Web browsers such as Netscape or Internet Explorer usually retrieve Web pages directly from the server where they are stored (revealing the user's IP address to the server) or from a cache run by their Internet Service Provider (usually generating logs on the ISP's system of all sites visited). A one-stage anonymiser such as *anonymizer.com* takes Web page requests and returns the requested page via an encrypted link with users. It also blocks further privacy-sensitive information travelling from the user to

---

154 Report of the Director of the Administrative Office of the United States Courts On Applications for Orders Authorizing or Approving the Interception of Wire, Oral, or Electronic Communications, April 2003. Available from http://www.uscourts.gov/wiretap02/2002wttxt.pdf

155 D. Chaum. Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. *Communications of the ACM*, 24(2) 84-88, February 1981.

Web servers. *Anonymizer.com* runs a Secure Tips Online Program[156] that allows anonymous tips about crime to be supplied to the FBI. The other technologies described in this section can be used to provide a similar service.

Anonymising systems such as *Crowds* add intermediate servers that receive encrypted requests from users, pass those requests through a small number of other servers and then on to the final destination before returning the requested Web page back the same way[157]. This design is meant to ensure that all of the servers on that route would need to be compromised to reveal the Web sites being accessed by a specific user.

More generally, systems have been designed to allow any type of Internet communication to be anonymous. These encrypt the "packets" that carry all types of Internet data and route them to their destination via a network of anonymising servers. Such systems could potentially allow all of the forms of communication now carried via the Internet to be carried on anonymously. *Onion routing* is one such experimental system that is in continuing development[158].

While anonymisers were a particularly active area of research and development in the late Nineties, they have yet to take off in the mass market. Running the anonymising servers to the high reliability standard required incurs hardware, bandwidth and maintenance costs. Policing abuse such as anonymous spam or harassing messages sent through anonymous mail servers requires a significant effort. Developing and updating user-friendly client software that integrates seamlessly with existing Web browsers, e-mail clients and other programs is a further cost.

Freedom was a commercial service from a Canadian company that had invested a large amount of venture capital in developing and running all of these elements of an anonymising IP service. The level of customer demand however proved to be entirely disproportionate to the continuing investment required in the high running costs, and the service was converted to a simple one-stage anonymising Web cache.

Anonymous payment mechanisms

Electronic payment mechanisms so far deployed have almost universally allowed the creation of detailed records of every transaction made. Financial institutions know exactly where, when and how much customers have spent using debit and credit cards. Online payment systems such as PayPal maintain similar transaction logs.

It might seem that electronic procedures to transfer money between two parties would necessarily allow a transaction record to be generated, even if there was a limit on how much information and for how long this record was stored. However, cryptographic techniques were developed in the 1980s to allow anonymous electronic tokens analogous to cash to be issued by banks, the operators of loyalty schemes and so on. While a bank can see that a customer has withdrawn a certain amount of "e-cash" from their account, and can later confirm that those electronic coins are still valid when they are spent, it cannot link the coins back to the original withdrawal[159].

So far, these anonymous payment mechanisms have failed to take off. There seems to be a general lack of consumer demand, without which few pieces of software have allowed customers to easily spend electronic cash or persuaded merchants to allow its

---

156 See http://www.anonymizer.com/tips/

157 M. Reiter and A. D Rubin. Crowds: anonymity for Web transactions. *ACM Transactions on Information and System Security*, 1(1) 66-92, November 1998.

158 M. G. Reed, P. F. Syverson and D. M. Goldschlag. Anonymous Connections and Onion Routing. *IEEE Journal on Selected Areas of Communication: Special Issue Copyright and Privacy Protection*, May 1998.

159 David Chaum. Blind Signatures for Untraceable Payments. *CRYPTO 82*, pp. 199-203.

use as payment. Patents on key parts of the techniques have also caused difficulties, although they will mostly expire within the timeframe considered by this paper[160].

However, not all "anonymous" cashless cards are in fact anonymous. In September 1995, Privacy International's Director Simon Davies investigated Mondex's claims that their digital cash service was "anonymous". Davies determined that, contrary to the Mondex public statements, in fact that the system was not anonymous and that the bank and merchants could find out the identity of the users.

Davies filed a Trade Descriptions Act complaint against Mondex for falsely advertising the service as anonymous. In June 1996, the Fair Trading Office responded noting that:

> *It appears the customer is identified to the trader, as in paragraph seven above and, ultimately, the bank, by the 300 previous transactions. Each of these will soon be superseded by further transactions and drop off the end of the list. These can be monitored by the bank and could be used for marketing purposes. This is the audit trail and ultimately could be sold to business users for third party marketing.*[161]

The office also noted that Mondex changed its literature and no longer claims that it was anonymous. The Office declined to press the issue further stating the online press releases were not covered by the act.

The Privacy International action did raise concerns that police and other bodies could gain access to detailed knowledge of a cardholder's purchases.

- o – O – o –

IB
London, February 2004

[160] Declan McCullagh. Digging Those Digicash Blues. *Wired News*, 14 June 2001. Available from http://www.wired.com/news/ebiz/0,1272,44507,00.html

[161] Complaint and background at http://www.privacyinternational.org/issues/mondex/

fipr

Foundation for Information Policy Research

UK INFORMATION COMMISSIONER STUDY PROJECT:

PRIVACY & LAW ENFORCEMENT

Paper No. 3:

TIA & PNR

February 2004

1. Introduction

This paper is the third of a set of papers exploring the implications of the use of new technologies for policing purposes, produced as part of a research project commissioned by the UK Information Commissioner into the question of Privacy and Law Enforcement. It deals with the US "Total/Terrorist Information Awareness" (TIA) system[162] and with the controversies over the transfer of airline passenger (PNR) data from the EU to the USA and over intra-EU proposals on the use of such data.

It is important to stress that the aim of this paper is not to analyse either the TIA system or the PNR controversies as such, and especially not to make specific policy proposals as to either of these. Rather, we are describing these matters as illuminating examples of the trend, throughout the western world, towards a surveillance culture driven, on the one hand, by the increased sense of threat from terrorist activity after the "9/11" attacks on the United States and, on the other hand, by a belief that technology can improve the effectiveness of law enforcement agencies, in particular in the area of intelligence-gathering and "preventive policing," more in particular (but not only) in relation to terrorism. The aim of this paper is to show, and critically discuss, the assumptions underpinning the TIA system and the demand for PNR data as part of that wider trend, and to contrast these with the findings in the other (combined) papers.

2. TIA and PNR in context

In Combined Papers Nos. 1 & 2, we have shown that over the last few decades there has been a major increase in the generation, retention and availability of personal data in many forms in both the public and the private sector, and an increased interest on the part of law enforcement agencies in the acquisition and use of such data. We also noted that this increased interest in personal data on the part of law enforcers was coupled with a move from responsive- to preventive policing, from crime investigation and "clear-up" to crime prevention and criminal intelligence gathering. And we noted that this latter trend constitutes a move toward surveillance and monitoring of potential threats and of persons categorised as possibly posing such a potential threat, even if there is as yet no evidence that they have committed, or are about to commit, a specific criminal offence.

More in particular, we identified the following dangers inherent in such new forms of intelligence-based "preventive policing:"

- the danger that data collected for certain purposes (e.g., marketing or credit scoring or travel), and which may be sufficient and sufficiently accurate for those purposes, are uncritically used for police purposes for which they are not suited and in respect of which they are may be unreliable; and

- the danger that individuals and groups of individuals are targeted for intrusive surveillance because they are deemed to be likely to present a future threat to the public peace or state security - with the assumptions underpinning such (tentative) predictions being (consciously or unconsciously) hidden in the (effectively unchallengeable) parameters which are set by those deciding on intelligence and surveillance priorities.

---

[162] The system was originally referred to as a "Total Information Awareness" system, but as discussed in the text below, at 3, this was later changed to "Terrorism Information Awareness."

This paper will show that these dangers are increased if the authorities, in their new intelligence-led activities, rely on relatively new and untested technologies. To this end, we will describe, in sections 3 and 4, the Information Awareness operation in the USA, and the issues surrounding the PNR controversy, and point out the underlying assumptions and inherent dangers in the programs[163] concerned - and against which, in the UK, the Information Commissioner is supposed to guard. In section 5, we will set out our conclusions.

3. "Information Awareness"

3.1 DARPA, the IAO, the TIA program and the TIA network

TIA was a program of the United States' Defense Advance Research Projects Agency (DARPA),[164] and more in particular of DARPA's Information Awareness Office (IAO), established in January 2002 in response to the events of 11 September 2001.[165] IAO's Mission Statement - like much else to do with the IAO and the TIA program - was formulated in rather dense jargon. It reads in part:

> "The DARPA Information Awareness Office (IAO) will imagine, develop, apply, integrate, demonstrate and transition information technologies, components, and prototype closed-loop information systems that will counter asymmetric [read: terrorist] threats by achieving total information awareness useful for pre-emption, national security warning, and national security decision-making." [166]

More specifically and somewhat more simply put, the aim of the IAO was:

> "to integrate advanced technologies [used in counter-terrorism] and accelerate their transition to operational users."[167]

IAO had two sections. One section consisted of "programs that develop technologies and components" - or rather, awards contracts to universities, commercial companies and government laboratories to perform the actual R & D.[168]

The other section was TIA. Basically, the first section of the IAO existed to develop programs for data collection and analysis, which fed into the second section, the TIA. However, TIA itself was also an R & D program.[169] Specifically, it was described as including:

---

163 Throughout this paper, we will use the American-English term "program" rather than the European-English term "programme," in particular to ensure consistency between the main text and quotes from US reports on the matters discussed. Otherwise, in the main text, we generally follow European-English usage.

164 According to DARPA's website: "*The Defense Advanced Research Projects Agency (DARPA) is the central research and development organization for the Department of Defense (DoD). It manages and directs selected basic and applied research and development projects for DoD, and pursues research and technology where risk and payoff are both very high and where success may provide dramatic advances for traditional military roles and missions.*" See: http://www.darpa.mil.

165 There are seven other "technical offices" within DARPA, apart from the IAO. IAO was created in close cooperation with the US Army Intelligence and Security Command (INSCOM)'s Information Dominance Center (since re-named the Information Operations Center). See: DARPA Report to Congress Regarding the Terrorism Awareness Program (above, footnote 4), *Detailed Information* (hereafter: *Detailed Information*), p. 1.

166 *Idem*.

167 *Idem*.

168 *Idem*.

169 See, e.g., the text under IAO's organogram on p. 2 of the *Detailed Information*, in which the TIA is listed as one of the programs.

> "a prototype network ... for integrating and testing [anti-terrorist] tools and concepts in an operational environment."[170]

In other words, there was a TIA program - which, in relation to the other programs, constitutes a "program of programs"[171] - the main component of which is the TIA network. In practice, and in the various reports on TIA, the terms "TIA program" and "TIA network" or "system" are often used interchangeably.

The TIA system had a number of "nodes" or terminals. The main one was located within the INSCOM Information Operations Centre.[172] There were further nodes designated for "subordinate INSCOM commands and other participating organizations from DoD [the US Department of Defence] and the Intelligence Community."[173] In other words, the (presumably, tentative) results coming out of the "test" TIA program would be fed directly to operational centres.[174]

In February 2003, the US Congress' House of Representatives partly suspended the financing of the TIA program pending the submission of a report on the program by DARPA.[175] This report was duly submitted to Congress on 20 May 2003 by the US Secretary of Defense, the Attorney General and the Director of Central Intelligence.[176] A joint House-Senate committee voted on 24 September 2003 to suspend funding for TIA during 2004, but allowed some of its research programs to continue under other government bodies such as DARPA and the National Foreign Intelligence Program[177]. For the purpose of this paper - using TIA and its original constituent research as an illustration of a wider trend - the exact current status of the program is however in any case not relevant.

3.2 Main features of the IAO and TIA program and network

"Information awareness" is, of course, just a new name for an old product. It used to be called "intelligence gathering and analysis." However, the US authorities clearly felt that there should be certain major shifts in the paradigms of this activity. The background, main features and ultimate goal of the "new, improved" product were summarised by DARPA as follows:

> "Today's intelligence infrastructure was designed for the Cold War and is well-suited to major military conflicts and strategic threats. However, our information about foreign terrorists is spotty at best – and our efforts to integrate and extend current intelligence information technologies are unlikely to yield adequate results in this new asymmetric threat environment. Foreign terrorists do not need to act in large numbers to cause great

---

170 *Detailed Information*, p. 1. The statement that the TIA network is used in an "***operational environment***" rather blurs the distinction between a (non-operational) "prototype" and a system that is actually used in practice: see the text. The same blurring can also be seen with regard to the CAPS-II system related to the use of PNR data, discussed below, at 4.

171 DARPA Report to Congress Regarding the Terrorism Awareness Program (above, footnote 4), *Executive Summary* (hereafter: *Executive Summary*), p. 1.

172 See footnote 7, above.

173 *Detailed Information*, p. 1.

174 See footnote 9, above.

175 See Subsection 111(b) of Division M of the Consolidated Appropriations Resolution, 2003 (Public Law 108-7), pp. 1118-1123. The full text of this resolution is attached as Attachment A.1.

176 Report to Congress Regarding the Terrorism Awareness Program, produced by DARPA in response to Consolidated Appropriations Resolution, 2003, Pub. L. No. 108-7, Division M, § 111(b), May 2003. The *Detailed Information* and the *Executive Summary* of this report, and the *System Description* of the TIA program produced separately by DARPA, provide the primary sources for this paper. They are attached as Attachments A.2 – A.4.

177 Stephen M. Cherry, Controversial Pentagon Program Scuttled, But Its Work Will Live On, IEEE Spectrum, September 2003.

damage, nor must they attack us frequently to influence us: they are low-density, low-intensity combatants. Commercial information technology provides foreign terrorists with cheap, effective communications, planning data, and command and control capabilities – as good as is available to most governments. The availability of biological and chemical weapons, in addition to novel methods of attack, poses a broad and continuing threat to the United States.

To address today's threat, we need to turn information technology around and use it against foreign terrorists, **making better use of existing, legally available information** so that we can predict and pre-empt attacks – or, at the very least, strike back with speed, certainty, and finality. We will need new technology for effectively managing all this information, for providing better access with improved controls, for improving the efficiency of data analysis, for communicating results to decision-makers, and for protecting the privacy of U.S. persons as well as the human and communication intelligence sources and methods used by intelligence agencies to collect information. **DARPA's research seeks to improve the interpretation of raw data using numerous automated and semi-automated technologies that amplify the efforts of human analysts to provide greatly improved attack prediction and pre-emption capabilities.** We also seek to multiply the value of existing information and analysis by **enabling cross-agency collaboration via technologies that rapidly assemble teams of authorized users to share and analyze legally collected information on foreign terrorist activities already in their possession**. DARPA's Information Awareness Office was established to create and integrate component technologies to address these varied needs and deliver a broader, more powerful set of tools to the intelligence community."

(DARPA Fact File: A Compendium of DARPA Programs, August 2003, p. 5, emphasis added)

"The ultimate goal is to create a counter-terrorism information architecture that:

(i) increases the information coverage by an order-of magnitude – via access and sharing, not by increased data collection – and that can be easily scaled;

(ii) provides focused warnings within an hour after a triggering event occurs or an evidence threshold is passed;

(iii) can automatically cue analysts based on partial terrorist threat-indicative pattern matches and has patterns that cover 90 percent of all known previous foreign terrorist attacks; and

(iv) supports collaboration, analytical reasoning, and information sharing so that analysts can hypothesize, test, and propose theories and mitigating strategies about possible futures, thereby enabling decision-makers to effectively evaluate the impact of current or future policies."

(DARPA Fact File: A Compendium of DARPA Programs, August 2003, p. 6)

It is clear from these quotes and from the general information issued by DARPA that the new system was intended:

(1) to draw in much more information, from many new sources (in particular also from the private sector, and worldwide), to select it, read it and make it much more quickly

available, in understandable, structured form, in English, to analysts and decision-makers, through new technologies which find, transcribe and if necessary translate and (pre-)digest the information for such users;

(2) to process and analyse this information in new ways, using (partly still-to-be-developed) new technologies; and

(3) to facilitate much greater cooperation between officials in different agencies, and much greater exchanges of information, ideas and hypotheses between such officials, unburdened by "top-down" bureaucratic obstacles.

It is useful to keep these three aspects of the whole "information awareness" operation separate, at least for an initial discussion (although there is considerable overlap between the first two in particular).

The main point to be made about the first aspect, the information-finding/collating/translating side of the operation, is that this is not limited to the more usual information obtained by the security services of the USA - or supplied to it by the secret services of other nations - such as "HUMINT" (human-sourced intelligence), results of the interrogation of terrorist suspects in Cuba, Afghanistan, Iraq or elsewhere, information from telephone intercepts and telephone traffic monitoring, etc., etc. – Although such information would of course also be fed into the TIA system.

Rather, the aim of TIA was to massively expand the information sources to be screened, with the aid of new (and often still-to-be-developed) technologies. The programs to develop these technologies were mainly situated in (or supported by) the first sector of the IAO (with the actually R&D being carried out by third parties, under contract), although use would undoubtedly also be made of non-IAO programs (such as the NASA program on a "non-invasive neuro-logic sensor" mentioned below).

As noted above, the aim was to increase the information collected and scanned for relevance "by an order of magnitude." The remark that this was to be done "via access and sharing, not by increased data collection" is disingenuous. Presumably, it is meant to indicate that the authorities have not proposed any further powers to collect data (in particular on U.S. citizens):

> "Nothing in the TIA program changes anything about the types of underlying information to which the government either does or does not have lawful access, nor does it change anything about the standards that must be satisfied for accessing particular types of data. TIA does not grant the government access to data that is currently legally unavailable to it. On the contrary, any deployment of TIA would have to operate within the confines imposed by current law."
>
> (*Detailed Information*, p. 32).

DARPA can give this assurance because, as it is put in the *Detailed Description*:

> "[an] enormous amount of data [is] already available to the government from classified and unclassified sources". (Appendix A, p. A-8)

This view, which assumes rather limited legal constraints on data collection and use, in particular as concerns non-US data and -databases, is further discussed below, under the heading "*not-very-limiting limitations*." Here, we must note that the emphasis in the system was:

(a) on extracting data from many different, disparate sources, public and private, open and secret, worldwide; and

(b) on quickly and comprehensively "covering" or "scaling" the "enormous amount" of data thus to be fed into the system.

Both rely heavily on new (or still-to-be-developed) technologies.

Thus, the **GENISYS** program (contracted to AlphaTech and its subcontractor, Oracle):[178]

> "aims to create technology that enables many physically disparate heterogeneous databases to be queried as if it was one 'virtually' centralized database. ... As a result, analysts would be able to access information much faster and with higher confidence in their results. They would be able to use all the databases to which they have access as a federation - a new 'megadatabase' would not be created."
>
> (*Detailed Information*, Appendix A, p. A-11).

The assurance in the above quote (and repeated elsewhere in this and other documents)[179] that TIA does not involve the creation of any new central database is thus again misleading: The system may not create a new, single database housed in a single physical mainframe computer. But it would create, in effect, a single new "virtual" one, more powerful than any 20th Century Big Brother computer could ever have hoped to be: this new technology would be let loose on basically any database or information-set to which the US authorities would have lawful access (with the "lawfulness" restriction being interpreted in a very narrow, US-centred way, as discussed below, under the heading "*not-very-limiting limitations*").

Also not particularly reassuring is the statement that TIA access to various databases does not extend to the manipulation of the data in such databases:[180] a person's privacy is invaded if the government accesses his bank account or medical file, irrespective of whether the government can change the details involved.

The official documentation is rather coy about the exact nature and sources of the "enormous amount of data" to be screened. From different passages, it is clear that DARPA aims to collect and screen both typical intelligence reports and -databases and much wider data sources. Thus, it says, first of all:

> "DARPA believes that to predict, track, and thwart attacks, the United States needs databases containing information about all potential terrorists and possible supporters;

---

178 For further detail of the **GENISYS** program, see *Detailed Information*, Appendix A, pp. A-10 – A-13; Fact File – A Compendium of DARPA Programs, p. 9.

179 Thus, it is stated in the *Detailed Information* that: "Further, the TIA Program is not attempting to create or access a centralized database that will store information gathered from various publicly or privately held databases." (p. 21). This sentence is repeated *verbatim* in the FAQs on TIA, set out on DARPA's website, in response to the question "Is TIA collecting data on US citizens?"

180 *Detailed Information*, p. 32, again repeated in the FAQs on TIA posted on DARPA's website.

> terrorist materials; training, preparation and rehearsal activities; potential targets; specific plans; and the status of our defenses."
>
> (*Detailed Information*, Appendix A, p. A-10)

But DARPA also says:

> "International terrorist organizations must plan and prepare for attacks against the United States at home and abroad, and their people must make transactions in carrying out these planning and preparation activities. Examples of transactions that may be of interest are activities such as telephone calls, travel arrangements, and the acquisition of critical materials to be used in their attacks. Data about these events may well be buried in an ***enormous amount of data about routine worldwide activity that has nothing to do with international terrorism***."
>
> (*Detailed Information*, Appendix A, p. A-3, emphasis added)

Elsewhere (in connection with the detection of misinformation through a program called MisInformation Detection, **MInDet**, discussed later), the *Detailed Information* document mentions "open-source information:"

> "Open source information may exist in news reports, web sites, financial reports, maritime registrations, etc. By its very nature, it is public information. At present, the Intelligence Community does not take full advantage of open sources, for a number of reasons. One reason is because of the sheer volume of open source information."
>
> (*Detailed Information*, Appendix A, p. A-17)

Otherwise, the documents merely refer to "other databases available to the Intelligence Community" (as distinct from the Intelligence Community's own intelligence reports and databases). One may assume that, with limitations on amounts that can be processed removed, the data to be "mined" may come to include, in particular, data contained in public (publicly accessible) registers and other open-source or commercially available databases outside the USA: electoral roll/population-register data, telephone-, fax-, and email-directories (and reversed versions of such directories), land registers, directories of companies and company officers, shareholder information, criminal records, court data, data from credit reference or direct marketing agencies, loyalty card information, etc.[181]

In many countries (in particular in Europe), the collection, transfer and use of such data is subject to significant restrictions under the relevant national laws applicable to such databases (including data protection laws) - but as discussed under the heading "*not-very-limiting limitations*," below, it is not entirely clear whether the US authorities feel bound by such restrictions. The basic assumption appears to be that as long as the US authorities can obtain access to the databases without violating *US* law, they could do so, and incorporate the databases in question into a new TIA "federation" of databases, with GENISYS ensuring (at some stage) that all these datasets could be accessed, compared and analysed as if they were contained in one single "mega database."[182]

---

[181] DARPA claims that its data analyses of such sources are quite different from the "data mining" performed by commercial companies, e.g. for direct marketing purposes: see below, in the discussion on the second aspect of the TIA process.

[182] We will discuss the legal issues this raises (also under the UK Data Protection Act) in our next paper, dealing with the legal framework for privacy and law enforcement.

TIA furthermore included a massive program to develop "biometrics-based human identification to recognize individuals and activities" and to capture the relevant data, in whatever format it is found: video, audio, photographic or whatever, with new technologies being used to link such data seamlessly with more traditional (text) formats of information, as noted below.[183] Unmentioned in the *Detailed Information* are two further programs, which go beyond mere identification to develop "the capability to automatically identify and classify anomalous or suspicious terrorist threat-indicative activities."[184]

To speed up the availability of any information in such sources in non-written form, in unstructured text and/or in foreign languages, new technologies are again being developed in various programs:[185]

> "Because of the volume of data that may need to be sorted through quickly and accurately, automated structured discovery methods will be developed. Data comes in many forms and languages. Voice data would be automatically transcribed to text to make it more easily searchable by machines. Foreign languages would be automatically translated into English. Unstructured text would be given some structure by identifying and extracting entities such as the names of people, places, things and events buried in the text so machines may process the volumes of text."
>
> (*Detailed Information*, pp. 3-4).

The "scaling" (initial relevance-assessment) of the data too is increasingly to be done by computers, rather than by human analysts:

> "Automated means of processing [the above-mentioned enormous amount of data] and converting it to relevant information would be a monumental task beyond the capabilities of the analysts without significant new applications of information technologies."
>
> (*Detailed Information*, Appendix A, p. A-8).
>
> "Today, the amount of information that needs to be considered far exceeds the capacity of the un-aided humans in the system. Adding more people is not necessarily the solution. DoD believes that there is a need to provide much more systematic, methodological approach that automates many of the lower-level data manipulation tasks that can be done well by machines guided by human users. Such an approach would, in turn, allow users more time for higher-level analysis that depends critically on a human's unique cognitive skills."

---

183 The main programs in this area are **HumanID** (Human Identification at a Distance), **ARM** (Activity, Recognition, and Monitoring) and **NGFR** (Next-Generation Face Recognition). For details see *Detailed Information*, Appendix A, pp. A-18 – A-22.

184 The programs are **HTID** (Human Threat Identification at a Distance) and **TARM** (Threat Activity Recognition and Monitoring). See Fact File: Compendium of DARPA Programs, p. 9. Other biometrics-based technologies being developed by the US authorities also extend beyond the identification of individuals: In July 2002, EPIC obtained documents under the US Freedom Of Information Act showing that NASA is developing so-called "**non-invasive neuro-logic sensors**" - a kind of brain scanner which its proponents claim will be capable of detecting the state of mind of a person (the report does not mention the undoubtedly catchy acronym for this program). This technology is not mentioned in the IAO documentation: it is apparently being developed in connection with airline passenger screening (further discussed below, at 4): see http://www.epic.org/privacy/airtravel/nasa. However, if it ever were to become a practical tool (which is rather unlikely in the foreseeable future), it could of course be linked to the TIA system: "nervousness" may well be a typical symptom of a terrorist on a mission (although how one would distinguish that nervousness from the nervousness of a passenger with a fear of flying is anybody's guess).

185 The main programs in this area are **EARS** (Effective, Affordable, Reusable Speech-to-Text), **TIDES** (Translingual Information Detection, Extraction, and Summarization) and **GALE** (Global Autonomous Language Exploitation). For details, see *Detailed Information*, Appendix B, pp. B-10 – B-16.

(*Executive Summary*, p. 2)

This aim was supported by a further program, **Genoa-II**, which sought to develop information technology, *inter alia*, to allow analysts to "Read Everything (Without Reading Everything)"[186]

> "This area includes the development of technology to help the analyst internalize and understand all the available information relevant to understanding the current situation without having to read all of it."
>
> (*Detailed Information*, Appendix B, p. B-3)

As the *Detailed Information* document points out, "structured discovery" - the above-mentioned machine-supported collection of structured and unstructured information, in many languages, and its collating - "is only the early stages of the process." Next comes the data analysis phase, which aims "to eliminate false leads, to refine the search and discovery process, and to establish a better understanding of terrorist intent."[187]

The basic approach is set out in the *Detailed Information* document as follows:

- Individuals suspected of involvement in terrorist activities would be identified through their physical presence and the transactions they make.
- Associations among such individuals and other key entities (e.g., other people, activities, events, transactions, and places) would be made.
- These associations would be linked with the associations of other individuals.
- Other types of intelligence would be melded [*sic*] into the developing picture of what is happening and false leads would be identified.
- The analyst would develop hypotheses about what these associates might be planning.
- The behaviour and activities of these associates may be introduced into models that are based on patterns of behaviour and activity that have been shown to be accurate or estimated to be predictors of terrorist attack.
- Based on these competing hypotheses, a range of plausible outcomes would be estimated and actionable options would be developed that address the maximum range of these plausible futures.
- A risk analysis would be done before the situation is presented to the decision-maker as early as possible so the decision-maker would have the maximum number of options to aid in deciding on a course of action or non-action.
- All the steps of this process would be recorded faithfully in a corporate memory (knowledge database) that would be helpful in the future in similar situations.

(*Detailed Information*, Appendix A, p. A-8).

---

186 The other aspects of Genoa-II relate to the second and third aspect of the Information Awareness project, and are discussed in those contexts, below.

187 *Detailed Information*, Appendix A, p. A-4.

Again, much of this was supposed to be done, or at least supported, by new technology. As we have seen, the identification of targeted individuals (first bullet-point) was to be facilitated through a variety of new technologies (HumanID, ARM, NGFR).[188] However, the official documents do not make clear how a person would come be classified as an "individual suspected of involvement in terrorist activities" in the first place. Rather, the description in the *Detailed Information* from which the above bullet-points are taken starts off with the model produced as a result of the above:

- Based on known vulnerabilities of the United States at home and abroad to terrorist attack and the known and estimated capabilities of the terrorist organizations, scenarios would be developed. The planning and preparation activities to carry out these attacks would be estimated taking into account the adaptations the terrorists would most probably make to counter our defenses. Those activities that may be observable as various kinds of data in the government databases available to the intelligence communities would be converted into subject- and pattern-based queries. This information would be pulled together into a model of a terrorist attack and made available to analysts.

- Using these models and other intelligence information as starting points, analysts would initiate automated searches of their databases. These models would be refined as additional information is obtained.

(*Detailed Information*, Appendix A, p. A-7)

Presumably, in building towards these models, the agencies involved would start off with identifying "known" terrorists and examining the associations between them and other persons. Such other persons would then (again presumably) be classified as "suspected of involvement in terrorist activities" if the associations reached a certain level or showed certain characteristics,[189] or eliminated as a "false lead" if there was clear information that the association in question was innocent (e.g., if the associate of the "known terrorist" was an undercover agent working for the US or its allies). In a way, it may therefore be supposed that the system is based on a feedback loop in which individuals caught up in the surveillance are continuously assessed for their appropriate classification.[190]

Thus, although the first models will have to be based on an analysis of known terrorists and past terrorist events, the idea is that those first models can then be used to discover activities and patterns corresponding to the model, through which as-yet-unknown terrorists and terrorist networks can be uncovered.

Again, this would be done by computer. The main program in this respect was called the Evidence Extraction and Link Discovery (**EELD**) program. It was described by DARPA as follows:

---

188 See footnote 21, above.

189 The German anti-terrorist agencies, who started (by today's standards, rather modest) programs of this sort (such as *Rasterfahndung*: searching by elimination) in the 1970s, used simple categories such as K1, K2, K3, etc. K1 were people who had regular or at least more than one-off contacts with "known terrorists," K2 were people who had such contact with people who had contact with "known terrorists;" etc. (The letter K stands for the German *Kontakt*).

190 In Germany in the 70s, lawyers representing persons accused of terrorist offences were automatically classified as K1 (and human rights activists such as Amnesty International researchers, who met the lawyers in that capacity, as K2). They were not automatically excluded: several lawyers in Germany were convicted of assisting the terrorist organisations of their clients. Customs officials on board trains entered the identity details of travellers onto a portable database. It was said that if a person happened to travel several times on the same train as a "known terrorist" or indeed as a "suspected terrorist" or a K2, this would lead to that person in turn being classified as K2.

> "The objective of the Evidence Extraction and Link Discovery (EELD) program is a suite of technologies that will automatically extract evidence about terrorist threat-indicative relationships between people, organizations, places, and things from unstructured textual data, such as intelligence messages or news reports. This information can then point to the discovery of additional, relevant relationships and patterns of activity that correspond to potential terrorist events, threats or planned attacks. These technologies would be employed to provide more accurate, advance warnings of terrorist activities by individuals and networks. They will allow for the identification of connected items of terrorist threat information from multiple sources and databases whose significance is not apparent until the connections are made. To avoid needless, distracting and unintended analysis of ordinary, legitimate activities, these technologies will also ensure that intelligence analysts view information about *only* those connected people, organizations, places, and things that are of counter-terrorist interest and concern, and which require more detailed analysis.
>
> In [Financial Year] 2002, EELD demonstrated: (i) the ability to extract relationships in several sets of text; (ii) the ability to distinguish terrorist threat characteristic, relevant patterns of activity from similar legitimate activities; and (iii) improvements in the ability to classify entities correctly based on their connections to *other* entities. These advances have been applied to significant intelligence problems on real data. In [Financial Year] 2003, the diversity of detectable relationships is being increased, the complexity of distinguishable patterns is being increased, and the ability to automatically learn patterns will be demonstrated. In [Financial Year] 2004, EELD will evaluate and transition selected components to the emerging Terrorism Information Awareness network nodes in the Defense and intelligence communities and will integrate the ability to learn terrorist threat-indicative patterns of interest with the ability to detect instances of those patterns.
>
> In summary, EELD develops technology not only for 'connecting the dots' that enable the U.S. to predict and pre-empt attacks, but also for deciding which dots to connect – starting with people, places, or organizations known or suspected to pose terrorist threats based on intelligence reports; recognizing patterns of connections and activity corresponding to scenarios of counter-terrorist concern between these people, places, and organizations; and learning patterns to discriminate as accurately as possible between real threats and apparently similar but actually legitimate activities."
>
> (Fact File: A Compendium of DARPA Programs, p. 7)

The crucial element in this description is the claim that EELD will not just look for patterns pre-specified by human analysts, but will also itself automatically "learn terrorist threat-indicative patterns of interest." DARPA believes that its computers will be able to discover "linkages among people, places, things and events," and can learn from these to develop "software algorithms to recognize patterns of relationships that are representative of terrorist groups."[191]

EELD was intended to become an artificial intelligence (AI) program which would, after an initial period during which it looked for pre-specified patterns, automatically "discover" new patterns, and would base subsequent alerts also on these new, computer-generated patterns.

---

191 *Detailed Information*, Appendix A, p. A-4.

This suggests that, at some stage, computers would *inter alia* suggest that a person should be regarded as "suspected of involvement in terrorist activities" on the basis of an algorithm generated by the computer itself. The explanation for this suggestion would be buried deep within the processes of the computer. Indeed, the patterns which the machine was supposed to discern were said (by DARPA) to be so complex as to be incapable of being simply expressed in words - which is why further technologies to visualise such unspeakably-complex patterns were under development (so-called "**Context Aware Visualization**").

Also notable is the reference to the program analysing "information from multiple sources and databases whose significance is not apparent until the connections are made" - in other words, the idea is that EELD would allow such "intelligent" searches and analyses through the entire "federation" of "databases available to the Intelligence Community." Furthermore, yet again, it is clear that this prototype system was already being used in actual operations.[192]

DARPA claimed that:

> "EELD techniques will also be useful in reducing false alarms because they would enable the explanation of certain patterns of activity as legitimate and, therefore, as unworthy of retention or investigation, separating these instances from those with no legitimate explanation or those whose participants are connected to known or suspected terrorists."
>
> (*Detailed Information*, Appendix A, p. A-14)

However, in addition, a separate program, MisInformation Detection or **MInDet**, was being developed, distinct from EELD. This program, already briefly mentioned above, sought to develop:

> "the ability to detect intentional misinformation and to detect inconsistencies in open source data with regard to known facts and adversaries goals. ... The motivating idea of MInDet is that automated determination of reliability of open sources will allow U.S. Intelligence to fully exploit these additional sources. Techniques will be developed for detecting misleading information in single documents, such as visa applications or maritime registrations as well as in a series of reports, e.g., news reports from different sources in a foreign country."
>
> (*Detailed Information*, Appendix A, p. A-17)

EELD also appears to build on an aspect of another program, **Genoa-II** (already mentioned above in connection with the first aspect of the Information Awareness effort and further discussed below, with reference to the third aspect of that effort: enhanced inter-agency cooperation). This is described as follows:

> "Evidential Reasoning, Scenario Generation, and Explanation. This area includes the development of structured argumentation and evidential reasoning tools that will help the analyst organize available data; generate hypotheses to understand the current situation;

---

[192] As it is put, rather obliquely (without an express reference to EELD) in the *Detailed Information*: "DARPA aims to develop techniques for detecting patterns that are based on known or estimated terrorist planning and preparation activities. Some of the prototype tools, which are applicable in these situations, are being developed in one of the IAO programs and ***early versions have been used by INSCOM analysts to help analyze captured data from Afghanistan and elsewhere***." Appendix A, p. A-4, emphasis added). For further details of EELD under the separate headings of Evidence Extraction (EE), Link Discovery (LD - "the core of EELD"), and Pattern Learning (PL), see *Detailed Information*, Appendix A, pp. A-14 – A-15. Note that the program was begun in 1999, before the establishment of the IAO and indeed before "9/11" (*idem*, p. A-14).

> generate possible futures that might develop from the current situation; generate and analyze possible interdiction options; and generate explanations of the analysis and reasoning process for decision-makers."
>
> (*Detailed Information*, Appendix B, p. B-2)

DARPA claims that its searching through large numbers of databases (including the "federation" of databases, mentioned earlier) is different from "data-mining" by commercial companies, e.g. for marketing purposes - which is why the tailor-made EELD program needed to be developed:

> "DARPA believes that EELD is needed because commercial data-mining techniques are focused at finding broadly occurring patterns in large databases, in contrast to intelligence analysis that consists largely of following a narrow trail and building connections from initial reports of suspicious activity. Commercial data-mining techniques are typically applied against large transaction databases, while intelligence needs to focus on a much smaller number of people, places, and things engaging in a far wider variety of activities. Commercial techniques attempt to sort all transactions and the people who make them into classes based on transaction characteristics; intelligence needs to combine evidence about multiple activities from a small group of related people. Patterns observed in commercial databases must be widespread to be of interest to companies; patterns that indicate activity of interest to the Intelligence Community are extremely rare. Commercial data mining combs many large transaction databases to discover predominant patterns; EELD technology combines information extracted from intelligence reports to detect rare but significant connections. The goal of the EELD research program is to extend data mining technology and develop new tools capable of solving intelligence problems; it is not performing data mining as the term is currently understood in the commercial sector."
>
> (*Detailed Information*, Appendix A, p. A-14).

The issues raised in this passage are further discussed in the assessment of the Information Awareness project, at the end of this section.

The third aspect of DARPA's Information Awareness program was a massive increase in inter-agency cooperation, again through new technology. As noted earlier, the TIA program is supposed to support, *inter alia*:

> "collaboration, analytical reasoning, and information sharing so that analysts can hypothesize, test, and propose theories and mitigating strategies about possible futures, thereby enabling decision-makers to effectively evaluate the impact of current or future policies."
>
> (Fact File - A Compendium of DARPA Programs, p. 6)

This aim was to be achieved by means of a further aspect of one particular program in particular: **Genoa-II** (already mentioned in relation to the other aspects of the Information Awareness effort, above). This aspect of Genoa-II is described as follows:

> "Collaboration and Corporate Memory. This area includes the development of computing infrastructure to enable distributed teams of analysts and decision-makers to form teams, share information and collaborate throughout the evidential reasoning,

> scenario generation, and explanation process. This technology needs to support collaboration at the 'edge' of very different organizations, while simultaneously allowing 'edge-to-center' collaboration between individual members of these groups and the 'center' of their home organizations."
>
> (*Detailed Information*, Appendix B, pp. B-2 – B-3).

In due course, this would combine with the two other aspects of Genoa-II, as follows:

> "Center-Edge Collaboration for Evidential Reasoning and Scenario Generation. During the next 18 months (3rd Quarter [of Financial Year] 2003 through 4th Quarter [of Financial Year] 2005), an enhanced suite of tools will be developed and evaluated. The evidential reasoning component will be enhanced to include tools for hypothesis comparison, argument critique, analogical reasoning, scenario generation, stochastic option generation, and storytelling.[193] The collaboration component will be enhanced tools to provide an initial center-edge collaboration environment, which will include context-based business rules, workflow management, SNA [Social Network Analysis] -based team management, consensus analysis, and knowledge-based security filters. The read-everything tools will provide alternative techniques for detecting and tracking content changes, relevant to the analyst's situation, in the incoming datastreams.
>
> Full Center-Edge Integration. During the last 2 years of the program (1st Quarter [of Financial Year 2006] through 4th Quarter [of Financial Year] 2007), a full center-edge collaboration environment with a full suite of evidential reasoning, scenario generation, and explanation capabilities will be developed and evaluated."
>
> (*Detailed Information*, Appendix B, p. B-3)

The impenetrability of this jargon should not obscure the implication of the program, which is that information, and speculation about information, will be much more widely shared within the "Intelligence Community." This may be a good thing in principle. However, it also significantly reduces the possibility for oversight and control. As it is put in a separate write-up of the program:

> "The collaboration component provides a basic peer-to-peer collaboration capability for organizations to form and manage *ad hoc* teams whose members are connected to one another along the edges of their parent organizations. These 'edge-to-edge' organizations eliminate traditional bureaucratic stovepipes found in top-down organizations, permitting workers to establish *ad hoc* groups to share and cooperate with their counterparts at other organizations."
>
> (Fact File - A Compendium of DARPA Programs, p. 6)

"Traditional bureaucratic stovepipes" in "top-down organizations" of course include safeguards against abuse and, in the context of data protection, against undue dissemination of

---

193 The term "stochastic" describes a process or system that is connected with random probability. The word "storytelling" is also a technical one, and "represents the capabilities for analysts and decision-makers to use storytelling and narrative techniques to communicate analysis output." DARPA encourages these techniques: "Conveying information in a story provides a rich context, remaining in the conscious memory longer and creating more memory traces than decontextualized information. Thus, a story is more likely to be acted upon than 'normal' means of communication. Storytelling, whether in a personal or organizational setting, connects people, develops creativity, and increases confidence. The use of stories in organizations can build descriptive capabilities, increase organizational learning, convey complex meaning, and communicate common values and rule sets." (*Technical Description*, para. 3.1.2.3.1.1, on p. 21).

information, and more in particular of highly sensitive personal information. DARPA does mention, shortly after the above, that:

> "The output of *ad hoc* teams operating along organizational edges must be reported back to management to allow for its inclusion in critical decision-making processes." (*idem*)

However, as a statement of serious concern, this is not very convincing. As we shall see under the next heading, the privacy safeguards listed in the DARPA documentation (and which again rely on computers rather than humans) are not very impressive.

3.3 Not-very-limiting limitations

The various reports and papers issued by the US authorities on the Information Awareness program stressed that the activities envisaged under it pose no threat to civil liberties because they are subject to certain constraints. In practice, these constraints are rather limited. Basically, they consist of three elements.

First of all, the reports stressed that the TIA system would only collect and analyse data that were already legally available to the relevant authorities, and that it would act in accordance with all relevant legislation. Secondly, they emphasise that the civil rights (and in particular the privacy) of U.S. citizens was not under threat. And thirdly, DARPA pointed to special oversight arrangements. It is worthwhile examining each of these supposed constraints separately (while noting the link between the first two in particular).

3.3.1 "Legally available information, lawfully used"

As already noted, DARPA stressed that:

> "Nothing in the TIA program changes anything about the types of underlying information to which the government either does or does not have lawful access, nor does it change anything about the standards that must be satisfied for accessing particular types of data. TIA does not grant the government access to data that is currently legally unavailable to it. On the contrary, any deployment of TIA would have to operate within the confines imposed by current law."
>
> (*Detailed Information*, p. 32).

Furthermore:

> "In its TIA work, as in all of its missions, the DoD must fully comply with the laws and regulations governing intelligence collection, retention, and dissemination, and all other laws, procedures, and controls protecting the privacy and constitutional rights of U.S. persons."
>
> (*Detailed Information*, p. 27)

To clarify the scope of such laws and regulations, the Congressional Research Service of the Library of Congress drew up a report on them.[194] In addition to the Fourth and Fifth

[194] Congressional Research Service, Report for Congress: Privacy: Total Information Awareness Programs and Related Information Access, Collection and Protection Laws, updated version, Library of Congress, March 2003 (hereafter: "*CRS Report*").

Amendments to the U.S. Constitution, this covered some 20 Federal statutes.[195] DARPA itself identified a further 8 Statutes, 3 Executive Orders, 8 Department of Justice Guidance/Orders, and 5 DoD Regulations and Guidance instruments.[196]

In its Report to Congress on TIA, DARPA stressed that it was not seeking any changes in the relevant statutes, or at least not in that report.[197] It may be noted that this does not exclude DARPA from seeking changes to the lower-level regulations, or to seek changes to statute law at a later stage. That however is not the main issue, nor do we propose to examine the current US laws and regulations mentioned in any detail. Suffice it to note that:

> "... federal law tends to employ a sectoral approach to the regulation of personal information ... These laws generally carve out exceptions for the disclosure of personally identifiable information to law enforcement officials and authorize access to personal information through use of search warrants, subpoenas and court orders. Notice requirements vary according to statute."
>
> (*Detailed Information*, p. 18, quoting *CRS Report*, p. 5, with approval)

In other words, US laws and regulations (like the laws and regulations in Europe) already contain broad exceptions allowing for the disclosure of personal information held by public and private bodies to law enforcement officials in certain circumstances, subject to certain procedural rules and safeguards. DARPA clearly accepted that, for the time being at least, these laws and exceptions gave sufficient scope to the "Intelligence Community" to obtain information which may be relevant to the Information Awareness effort.[198]

In a way, however, this is beside the point. This is because that effort is mostly directed at information and databases that are (or are assumed to be) ***outside the scope of the above-mentioned US laws and regulations***. Specifically, DARPA stresses that the Information Awareness tools which are the focus of privacy concerns (specifically, its EELD program):

> "are being applied only with respect to foreign intelligence data."
>
> (*Detailed Information*, p. 31)

The assumption appears to be that such "foreign intelligence" consists of (or at least stems from) information and databases outside the US and that it does not include information on US citizens - although it is accepted that if they did include such information, this would raise legal issues:

> "Any agency contemplating deploying TIA's search tools for use in particular contexts will be required to conduct a *pre-deployment legal review* of whether the contemplated deployment is consistent with all applicable laws, regulations, and policies. ***Some particular deployments, for example, might only be legally permissible if the tools developed had been shown, as a technological matter, to properly avoid retrieving data on U.S. persons, whether through anonymization techniques or otherwise***."

---

195 See the list in *Detailed Information*, p. 19 and the additional statutes referred to at the top of p. 20.
196 See *Detailed Information*, pp. 20 – 26.
197 *Detailed Information*, p. 28
198 In many European States, statutory exceptions for the benefit of law enforcement agencies and -activities are not applicable to the intelligence services, which benefit from separate exceptions to protect national security etc. It would appear that in the USA this distinction is not as significant.

> (*Detailed Information*, p. 34, original italics in the second line; emphasis on last sentenced added)

This absence of protection for non-US citizens is further discussed under the next sub-heading. Here, it may suffice to note that ***it appeared to be assumed that, as long as TIA did not involve data on US persons, the data processed under it were not subject to the US laws and regulations mentioned.***[199] Since, as we have seen, it is exactly on data on non-US citizens that the effort is focussed, this means that the long list of laws and regulations supposedly adhered to by DARPA in these activities, is largely meaningless.

The question of whether the collection of personal data under the Information Awareness program in other countries, the transfer of such data to the USA, and the use of such data in the USA, might be subject to the laws of those other countries is, as far as we can see, not even asked, let alone answered. ***There is no indication anywhere in the US Government's reports and statements that it feels constrained in its Information Awareness activities by the data protection- or other laws of other States***.

3.3.2 Protecting the rights of U.S. citizens: the *Guantanamo Bay*-approach to human rights and privacy

To us (as Europeans), one of the most striking features of the assurances given by the US authorities in respect of the Information Awareness effort, is the almost mantra-like statement that the program does not threaten "the privacy and the civil liberties ***of U.S. persons***:"

> "Safeguarding ***the privacy and the civil liberties of Americans*** is a bedrock principle."
>
> "In its TIA work, as in all of its missions, the DoD [Department of Defense] must fully comply with the laws and regulations governing intelligence collection, retention, and dissemination, and all other laws, procedures and controls protecting ***the privacy and constitutional rights of U.S. persons***."
>
> "TIA is seeking to develop new technologies ... that will safeguard ***the privacy of U.S. persons*** ..."
>
> (*Detailed Information*, pp. 27 and 28, emphasis added; these claims are repeated *verbatim* in the *Executive Summary*, p. 3, and in the FAQs; similar assurances are given in many other passages.)

This is not some unintentional slip of the tongue, caused by a focus on the US audience of the reports: it is a conscious distinction. Thus, DARPA says elsewhere that TIA-related programs involving data access, data search and pattern recognition involve:

> "technologies which, ***if applied to data on U.S. persons***, would raise serious issues about privacy."
>
> (*Detailed Information*, p. 3, emphasis added).

Or even more starkly:

---

[199] The documentation tends to refer to "U.S. persons" rather than U.S. citizens. Presumably, this is to avoid any suggestion that the Information Awareness tools might be used against illegal immigrants.

> "***To the extent that TIA's search tools would ever be applied to data sources that contain information on U.S. persons***, the privacy issues raised by these tools are significant ones that would require careful and serious examination."
>
> (*Detailed Information*, p. 33, emphasis added)

The answer, in DARPA's view, is simply to adopt measures to ensure that databases which mainly contain data on US citizens are not routinely accessed, and that, to the extent that data on US citizens were to be stumbled upon in non-US databases, the privacy concerns can be eliminated by not using such data (or only using them subject to special approval). DARPA thus stressed, in an apparent attempt to stave off criticism, that:

> "The EELD automated toolset, once developed, will assist intelligence analysts by automatically drawing to their attention the key relationships among subjects of lawful investigations drawn from the materials currently gathered and reported ***about non-U.S. persons*** ..."
>
> (*Detailed Information*, Appendix A, p. A-14, emphasis added)

The same is clear from the paragraph about the obligatory "*pre-deployment legal review*" for TIA techniques, quoted under the previous sub-heading.

It was to underline this approach, this distinction in treatment between US- and non-US individuals, which led DARPA to change the name of its project from "Total Information Awareness" to "Terrorism Information Awareness:"

> "This name ["Total Information Awareness"] created in some minds the impression that TIA was a system to be used for developing dossiers on US citizens. That is not DoD's intent in pursuing this program. Rather, DoD's purpose in pursuing these efforts is to protect U.S. citizens by detecting and defeating foreign terrorist threats before an attack. To make this objective absolutely clear, DARPA has changed the program name to Terrorism Information Awareness."
>
> (*Executive Summary*, p. 1, footnote 1. This statement is repeated, almost *verbatim*, in the FAQs on TIA, posted on DARPA's website)

DARPA failed to recognise that if its data-collecting and analysing activities raise serious concerns if applied to US citizens, they raise the same concerns if applied to non-US citizens. It is one of the main achievements of modern (post-World War-II) international human rights law that it provides guarantees to all persons affected by a State's actions - rather than just to that State's nationals or to the nationals of the other States Party to the relevant instrument. Just as it is unacceptable that the USA refuses to extend the protection of its own Bill of Rights (or of the UN International Covenant on Civil and Political Rights to which it is a Party) to individuals it holds in a camp outside its geographical territory, in Guantanamo Bay in Cuba, so it is also unacceptable that it refuses to protect the privacy of non-US individuals whose data it deliberately collects and analyses.

3.3.3 Quis custodiet ipsos custodes? The custodians themselves (with the help of a computer)!

The safeguards against human rights violations that might result from the deployment of TIA programs were summarised in the FAQs posted on DARPA's website as follows:

> "The Secretary of Defense will, as an integral part of oversight of TIA research and development, continue to assess emerging potential privacy and civil liberties impacts through an oversight board composed of senior representatives from DoD and the Intelligence Community, and chaired by the Under Secretary of Defense (Acquisition, Technology and Logistics). The Secretary of Defense will also receive advice on legal and policy issues, including privacy, posed by TIA research and development from a Federal Advisory Committee composed of outside experts.
>
> The Department of Defense has expressed its intention to address privacy and civil liberties issues squarely as they arise, in specific factual and operational contexts and in full partnership with other Executive Branch agencies and the Congress. The protection of privacy and civil liberties is an integral and paramount goal in the development of counterterrorism technologies and in their implementation
>
> DoD has expressed its commitment to the rule of law in this endeavor and views the protection of privacy and civil liberties as an integral and paramount goal in the development of counterterrorism technologies."
>
> (with reference to *Executive Summary*, p. 5, and *Detailed Information*, p. 35)

It may suffice to note that this is a purely internal supervisory system: the oversight board is composed entirely of DoD and Intelligence insiders and chaired by a politician. The only outside input is by "experts" appointed by the Executive; there is no guarantee of independence; and in any case they can only provide advice. This system does not constitute what in European legal terms would be called an "effective remedy" or safeguard against abuse.

Furthermore, the oversight will of course be limited to ensuring compliance with US laws and regulations insofar as data on US persons is concerned, in accordance with the limitations noted earlier.

In addition:

> "TIA is seeking to develop new technologies, including Genisys Privacy Protection, that will safeguard the privacy of U.S. persons by requiring, documenting, and auditing compliance with the applicable legal requirements and procedures."
>
> (*Detailed Information*, p. 27, repeated *verbatim* in the FAQs)

The **Genisys Privacy Protection** program was not solely concerned with privacy. Thus, first of all, it sought to:

> "research and develop new technologies to ensure personal privacy and protect sensitive intelligence sources and methods in the context of increasing use of data analysis for detecting, identifying, and tracking terrorist threats. ... Americans are rightly concerned that data collection and analysis activities by the Intelligence Community threaten their privacy. To address this concern, the Genisys Privacy Protection Program will conduct R&D on technologies that enable greater access to data for security reasons while protecting privacy by providing critical data to analysts while not allowing access to

> unauthorized information, focusing on anonymized transaction data and exposing identity only if evidence warrants and appropriate authorization is obtained for further investigation, and ensuring that any misuse of data can be detected and addressed.
>
> If successful, Genisys Privacy Protection will develop algorithms that prevent unauthorized access to sensitive identity data using statistical and logical inference control. This privacy protection technology would be used to develop roles-based rules for distinguishing between authorized and unauthorized uses of data and will automate access control. The program will also seek to improve the performance of algorithms for identity protection by limiting inference from aggregate sources. ...
>
> Access to Government databases today is granted ad hoc by system administrators. Thus, access is non-standard, slow, and often not granted unless direct interaction is mandated. Terrorists have already exploited the inability to share information and act collaboratively on problems. Role-based access control using standardized business rules would automate access appropriately, in a controlled and well-understood manner. ..."
>
> (*Detailed Information*, Appendix A, p. A-12)

In view of our earlier observations and the express reference in the above quote (again) to the concerns of "Americans" only, it is, we believe, not unduly paranoid to fear that the denial of access to "unauthorized data" in the above quote means denying the Intelligence Agencies access to data on *US* persons, if to provide such access would be contrary to *US* law; that only data on *US* persons will ever need to be anonymised; that authorization will only be needed for access to data on *US* persons; that only the drawing of inferences from aggregate data on *US* persons would be subject to algorithm-based limitations; and that, in effect, the system would guard only against such narrowly-defined exigencies.

This would agree with the remark in the quote at the bottom of page 17, above, that certain activities could be allowed as long as "tools [had been] developed ... to properly avoid retrieving data on U.S. persons, whether through anonymization techniques or otherwise."

The last paragraph in the above quote is perhaps the most revealing. It suggests that the automated Genisys Privacy Protection program would actually allow *greater access* to data than is granted by human system administrators.

This is only counterbalanced by the suggestion that highly-sophisticated tools are to be developed to keep a trail of all data uses. As the documentation points out:

> "This technology may have utility not only for personal privacy, but also for the intelligence insider threat."
>
> (*Detailed Information*, Appendix A, p. A-12)

3.4 Assessment

As we have seen, the Information Awareness program was to lead to a situation in which computers automatically:

- ✓ identify individuals, including persons previously classified as suspected terrorists and "associates" of suspected terrorists, also from a considerable distance;[200]

- ✓ scan "enormous amounts" of data in disparate, heterogeneous databases in public and private hands, worldwide; identify and select relevant information from this "virtual megadatabase" while discarding irrelevant information; and turn the relevant information into easily-understood (text-based) information where necessary;

- ✓ recognise patterns in the above information correlating to patterns of activity associated with previous terrorist activities, and on this bases:

- ✓ identify activities regarded as possibly indicative of terrorism; and

- ✓ further classify (or de-classify) individuals as "persons suspected of involvement in terrorist activities" (suspected terrorists) or as "associates" of such persons;[201]

- ✓ automatically construct new patterns of activity associated with terrorist activities from the application of the earlier patterns and additional information ("learning"), and searching for such new patterns; and

- ✓ alert intelligence analysts and political decision-makers to the whereabouts and activities of persons (previously or newly) classified as terrorist suspects or associates, and to activity corresponding to (new, improved) patterns - with the underlying basis for the new patterns being so complex that it can only be expressed in non-textual "visualizations".

The effective deployment of such a system rests on a number of assumptions:

- ✓ that computers can reliably identify individuals and activities at a distance;

- ✓ that computers can reliably weed out "relevant" information from "enormous amounts" of innocuous information - which in turn assumes that computers can reliably assess the relative accuracy and reliability of the data in the different datasets (which includes, but is not limited to, the capacity reliably to identify deliberate misinformation);

- ✓ that computers can be relied upon to accurately translate information from foreign languages (including the vast range of Arabic and Central-Asian languages and dialects) into English and to accurately turn non-text-based information into text;

- ✓ that computers can be relied upon to accurately discern pre-specified patterns in very large datasets;

- ✓ that the new patterns created by computers are reliable indicators of who may be a terrorist (or a potential terrorist, or a possible supporter of a potential terrorist), and of actual or possible terrorist activity; and

---

[200] It is important to avoid a semantic confusion in this context. Documents often refer to the "identification" of (say) suspected terrorists, when they mean that a particular individual is deemed to be a terrorist, i.e. that he must be classified as a terrorist (or as a suspected terrorist, or as an associate of a suspected terrorist, or whatever). This should not be confused with "identifying" a suspected terrorist in the sense of confirming that a particular person is a particular person: that John Blocks is the terrorist John Blocks (and not the entirely different person, John Blogs, or even a different John Blocks).

[201] See the previous footnote.

- ✓ that analysts and decision-makers can retain control over such automated processes, and can effectively re-appraise the relevant computer-based conclusions.

There are two key issues here: **reliability** and **control**.

Even such (in concept) relatively straight-forward ideas as automated face-recognition and translations of foreign text are at present not all that reliable. Such unreliability is greatly compounded if the technology is moved to a higher cognitive level. Computers are pretty good at detecting straight-forward, pre-specified patterns of fact. But they are much less reliable in assessing vaguely defined patterns which may (or may not) suggest that a particular, complex event may occur.

It has been pointed out that even extremely small margins of error would, in this context, be unacceptable in a democratic society. As it was put in a letter from the U.S. Public Policy Committee of the Association for Computing Machinery (the leading non-profit membership organization of computer scientists and information technology professionals in the USA) to the Chairman of the Senate Committee on Armed Services:

> "Because TIA would combine some types of automated data-mining with statistical analysis, there would be a significant personal cost for many Americans. Any type of statistical analysis inevitably results in some number of false positives - in this case incorrectly labeling someone as a potential terrorist. As the entire population would be subjected to TIA surveillance, even a small percentage of false positives would result in a large number of law-abiding Americans being mistakenly labeled. ... Research to increase accuracy and eliminate false positives in such systems is clearly worthwhile, but the rate can never be reduced to zero while maintaining some functionality. Is any level of false positive acceptable - and Constitutional - in such a system?
>
> The existence of TIA would impact the behavior of both real terrorists and law-abiding individuals. Real terrorists are likely to go to great lengths to make certain that their behavior is statistically 'normal,' and ordinary people are likely to avoid perfectly lawful behavior out of fear of being labeled 'Un-American.'
>
> To summarize, we appreciate that the stated goal of TIA is to fund research into new technologies and algorithms that could be used in a large surveillance system in the service of eliminating terrorist acts. However, we are extremely concerned that the program has been initiated and some projects already funded apparently without independent oversight and without sufficient thought being given to real constraints - technical, legal, economic, and ethical - on project scope, development, field testing, deployment, and use. Consequently, the deployment of TIA, as we currently understand it, would create new risks while having an unknown effect on overall security."
>
> (Letter from the U.S. Public Policy Committee of ACM to the Chairman of the Senate Committee on Armed Services, 23 January 2003)

We will leave aside the fact that the authors of the above letter share the authorities' focus on the rights and interests of US citizens: the basic analysis is equally true if applied to non-US persons. Indeed, the margin of error will be much higher when the TIA programs are applied to non-US data in foreign languages, culled from databases in developing countries.

Furthermore, the comments in the *Detailed Information* document, contrasting TIA data analysis of large datasets with commercial "data mining," quoted above, suggest that, if anything, the margin of error in the TIA programs would be much higher than those in such commercial endeavours - and the latter show considerable margins of error. These are acceptable in that context because the users are content with modest results. In direct marketing, a response (*success*) rate of 10% is high. In intelligence, as we have just seen, a *failure* rate of 10% (or even 1%) would be utterly unacceptable.

In addition, we have great doubts as to the feasibility of computers automatically learning to define reliable new patterns in the contexts concerned. The margin of error inherent in such patterns will be unacceptably high - and this will not be manifest until the patterns have been applied to large numbers of innocent people, with many being singled out for what will later transpire to have been totally unjustified surveillance and restrictions. If computers are allowed to create such new patterns, these will moreover reflect inherent biases, consciously or unconsciously built into the program used for such "learning" and pattern-definition.[202]

One inherent factor affecting the reliability of programs such as EELD (which also affects the reliability of human intelligence officials) is the ill-defined nature of the target of the searches. The documents say that the United States needs comprehensive information about "all potential terrorists and possible supporters." It is difficult enough to find out who is a real terrorist. To try and classify an individual as a *potential* terrorist is much trickier. And targeting *possible supporters of potential terrorists* casts the net extremely wide. How can one ever measure the reliability of such a speculative classification? Whenever human agents (State officials) have tried to classify individuals on such a basis, they have targeted large numbers of law-abiding citizens, typically on the basis that some of their lawful activities (like peaceful protest) could be regarded as potentially supportive of other individuals who might resort to violence in pursuit of the same aims. Computers could not improve on this: the unreliability is embedded in the vagueness of the class to be targeted. However, computer-aided classification would lend an entirely spurious air of objectivity and reliability to the exercise. Individuals will find it impossible to find out why they are classified in a particular way (as mentioned above, the underlying pattern is supposed to be so complex as to be unexpressable in ordinary language), let alone argue that the classification is wrong.

In addition, the massive programs involved in TIA would likely lead to an increase, not just in data collection, but also in data retention. This is clear from the quote given earlier, about the EELD program being able to separate "legitimate activity" from "instances with no legitimate explanation or those whose participants are connected to known or suspected terrorists:" it suggests that information on an event, and on persons involved in an event, would be retained unless a "legitimate explanation" for the event, or for their presence, is deemed to exist. In case of doubt, data are to be retained. Even more worrying, it suggests that information on perfectly legitimate activities would still be retained if those participating in the event (say, a demonstration) are believed to be "connected to known or suspected terrorists." That clearly again casts the net extremely wide. If (as is increasingly done in Europe) one were to classify violent anti-globalisation protesters as "terrorists" (because they are organised and use

---

202 Cf. the observation with regard to police CCTV surveillance of public areas in the UK that "*both suspicion and [police] intervention are socially constructed*" and are selectively targeted on "*social groups which [the CCTV operators] believe most likely to be deviant*", which leads to "*over-representation of men, particularly if they are young or black*" (Norris & Armstrong: The Maximum Surveillance Society - the Rise of CCTV, Oxford & New York, 1999).

violence for political ends, even if this is against property), it would allow for the retention of data on anyone who attends a demonstration also attended by such violent protesters.
All this is the more worrying in view of the serious implications which can flow from being classified as a "suspected terrorist" (or even as an "associate"). Even if one leaves the most extreme consequences of arrest, detention or even assassination aside,[203] it can entail a person being denied a job, being subjected to intrusive surveillance, in-depth questioning, or being stopped from boarding airplanes on the basis of a colour-coded "flag" on a list.

All this calls for the most stringent controls. Yet, as we have seen, such restrictions as proposed were extremely limited. There are few, if any controls on the collecting, transfer to the USA, and analysis in the USA, of (even highly sensitive) "foreign intelligence information" or data culled from "open source" material and databases outside the USA. The US authorities appear to feel that the restrictions on data processing, set out in US laws and regulations, do not apply to such foreign data and databases; and there is no indication that they seek to comply with any non-US laws that might apply to such matters. Non-US persons whose data may be subject to the TIA programs are effectively left in a legal "*Guantanamo Bay*"- style legal limbo: their privacy and data protection interests are denied.

The supposedly highly-sophisticated automated Privacy Protection Program would appear, in effect, to again protect only US citizens, and would indeed even for them allow *greater access* to data than is granted by human system administrators.

Such administrative controls as proposed were furthermore limited to internal bureaucratic oversight by senior executives of the very agencies to be scrutinised, under the chairmanship of a politician.

In sum, in spite of the grave dangers inherent in the TIA system and programs, there were no real and effective remedies against abuse.

4. The PNR data controversies[204]

4.1 Introduction

In the aftermath of the events of 11 September 2001, the United States adopted a number of laws and regulations requiring foreign airlines flying into their territory to transfer to the US administration personal data relating to passengers and crew members flying to or from this country. In particular, US authorities imposed on airlines the obligation to provide the US Bureau of Customs and Border Protection (CBP) with direct electronic access to passenger data contained in the Passenger Name Record (PNR) for flights to, from, or through the US. Airlines not complying with these demands may face heavy fines and even loss of landing rights, as well as seeing their passengers subject to delays on arrival in the US.

These US demands caused (and continue to cause) serious political and legal concern in the European Union. EU law imposes strict limitations and conditions on the transfer of personal

---

[203] Cf. the recent attack by US forces on a car in Yemen, in which five persons, believed (by the US) to be terrorists, were assassinated ("the subject of targeted killing").

[204] For full details on the matters discussed here, see Privacy International, Transferring Privacy: The Transfer of Passenger Records and the Abdication of Privacy Protection - The first report on 'Towards an International Infrastructure for Surveillance of Movement', February 2004; Edward Hasbrouck, "Total Travel Awareness:" Travel Data and Privacy, published on the author's website: : http://hasbrouck.org/articles/travelprivacy.html#TIA; and the dedicated Statewatch websites http://www.statewatch.org/pnrobservatory.htm and http://www.statewatch.org/eu-pnrobservatory.htm.

data (and especially of sensitive personal data) to "third" (i.e. non-EU) States that do not provide for an "adequate" level of data protection, comparable to the level of protection guaranteed in the EU. The USA does not provide such general protection. Personal data may therefore, in principle, not be transferred to that jurisdiction from any EU (and EEA) State, unless certain limited exceptions apply. A special arrangement under which personal data may be transferred to private companies and organisations in the USA which publicly promise to provide proper protection (the so-called "Safe Harbor") cannot be extended to the PNR data transfers required by the above-mentioned US laws and regulations.[205]

Rather, if the transfers are to be made lawful, other special arrangements will have to be made. The European Commission has been involved in lengthy and difficult negotiations with the US authorities with the aim of obtaining binding undertakings from the US authorities to address the issues. The Working Party established under Art. 29 of the main EU Directive on data protection (Directive 95/46/EC), which consists of representatives of the data protection authorities of the EU (and EEA) Member States and which formally advises the European Commission on such matters, has issued several opinions on the matter,[206] and the European Parliament has also closely, and critically, followed the negotiations.[207]

The latest developments are that on 16 December 2003 the Commission declared to Parliament that it felt that it could issue an "adequacy" finding under Article 25(6) of the EC Directive, on the basis of "undertakings" it expected to be given by the CBP.[208] On 12 January 2004 these undertakings were submitted by the USA. They were not officially made public at the time but were leaked and published on a number of websites of privacy- and human rights advocates. Although the Commissioner responsible, Frits Bolkestein, wrote to his US counterpart in the discussions, Tim Ridge, Secretary of the US Department of Homeland Security, that the "initial reaction from Members of the European Parliament was relatively balanced," many MEPs expressed continuing concern. This concern was given strong backing by the Working Party which, on 29 January 2004, issued its latest opinion on the matter (Opinion 2/2004). In this Opinion, the Working Party made clear that, in its view, the Commission should not issue a formal "finding" to the effect that the US undertakings provided "adequate" protection, unless it obtained substantial further clarification and stronger guarantees.

In this, the Working Party referred to another opinion, issued just two weeks earlier, in which it held that the arrangements made for the transfer of such data to Australia *were* "adequate" (Opinion 1/2004).[209] Clearly, the Working Party felt that the EU-USA arrangements should

---

205 For details on the complex issues involved (including the question of how to assess "adequacy" and an extensive discussion of the "Safe Harbor"), see Chapter 7, *Transborder data transfers*, in: D Korff, The EU Laws on Data Protection, FEDMA (Brussels) and DMA-USA (Washington), March 2004.

206 See WP66 of 24 September 2002, containing *Opinion 6/2002 on transmission of Passenger Manifest Information and other data from Airlines to the United States*; WP78 of 13 June2003, containing *Opinion 4/2003 on the Level of Protection ensured in the US for the Transfer of Passengers' Data*; WP87 of 29 January 2004, containing *Opinion 2/2004 on the Adequate Protection of Personal Data Contained in the PNR of Air Passengers to Be Transferred to the United States' Bureau of Customs and Border Protection (US CBP).*

207 See the European Parliament Resolutions of 13 March and 9 October 2003 and the debates on these resolutions.

208 Frits Bolkestein, Member of the European Commission in charge of the Internal Market, Taxation and Customs, Address to European Parliament Committees on Citizens' Freedoms and Rights, Justice and Home Affairs and Legal Affairs and the Internal Market on *EU/US talks on transfers of airline passengers' personal data*, Strasbourg, 16 December 2003 (speech/03/613).

209 WP85 of 16 January 2004, containing *Opinion 1/2004 on the level of protection ensured in Australia for the transmission of Passenger Name Record data from airlines.*

be inspired by the EU-Australian ones (although the legal situation in the two "third countries" is rather different).[210]

Whether the Commission will try to re-open the issues raised by the Working Party and MEPs or whether it will go ahead with an "adequacy" finding without further undertakings from the USA is still unclear at the time of writing (early-February 2004).[211]

In the meantime, the Commission and the Irish Presidency have recently proposed that the EU should develop its own policy on the disclosure of PNR data to EU (and Member States') law enforcement authorities. This is to include a *centralised data system*. Furthermore, on the basis of the principle of reciprocity, the Commission is now arguing that the system should be globalised through discussions within ICAO, the International Authority for Civil Aviation (a UN body).[212]

This turns on its head the concern expressed by the Working Party that if the demands of the US authorities were granted, the latter would have powers of access to data held in the EU and/or on EU citizens:

> "... that exceed the powers currently granted to European judicial and police authorities and/or authorities in charge of immigration matters or even of intelligence and security services when carrying out similar activities in the European Union." (WP78, p. 5)

Rather than seeking to limit the powers demanded by the US, the Commission is responding by seeking to extend the powers of the EU authorities.

In the next sub-sections, we will briefly discuss the main issues raised by the use of PNR data for law enforcement purposes (in the broadest sense, including anti-terrorism) and the special issues of the use of PNR data in the US CAPPS II system and the link between PNR, CAPPS II, and TIA.

4.2 The issues raised in connection with the transfer and/or use of PNR data

4.2.1 General issues

The first point to be noted is the inherent sensitivity of passenger travel data (irrespective of whether the data include the "special categories of data" listed in Art. 8 of the Framework Directive):

> "Passenger Name Records (PNR's) maintained by airlines, computerized reservations systems or 'global distribution systems' (CRS's/GDS's), and travel agencies don't just

---

210 Cf. the comment by the Working Party in WP87, quoted in the *Assessment*, below, that "that the recent experience of certain countries, such as Australia, shows that the legitimate requirements of internal security and fight to terrorism can be pursued in a proportionate and reasonable way through systems which are in line with the fundamental principles of privacy and data protection."

211 If the Commission does go ahead with an "adequacy" finding without changes to the arrangements, it could face a legal challenge from Parliament or, in due course, from a passenger whose data were transferred under the arrangement. Parliament would have to show that the Commission used its powers wrongly, while an individual could challenge the compatibility of any "adequacy" finding with the Framework Directive (on the basis that the Commission "finding" was contrary to the facts and to the criteria for judging "adequacy" set out in the Directive, as elaborated on by the Working Party), and/or to the European Convention on Human Rights and "general principles of Community [and indeed Union] law" (and perhaps the Charter if incorporated in the Convention in a legally binding way). Both avenues raise complex legal questions which need not be further discussed here.

212 See Privacy International, Transferring Privacy (footnote 43, above).

> contain flight reservations and ticket records. They include car, hotel, cruise, tour, sightseeing, and theater ticket bookings, among other types of entries.
>
> PNR's show where you went, when, with whom, for how long, and at whose expense. Behind the closed doors of your hotel room, with a particular other person, they show whether you asked for one bed or two. Through departmental and project billing codes, business travel PNR's reveal confidential internal corporate and other organizational structures and lines of authority and show which people were involved in work together, even if they travelled separately. Particularly in the aggregate, they reveal trade secrets, insider financial information, and information protected by attorney-client, journalistic, and other privileges.
>
> Through meeting codes used for convention and other discounts, PNR's reveal affiliations -- even with organizations whose membership lists are closely-held secrets not required to be divulged to the government. Through special service codes, they reveal details of travellers' physical and medical conditions. Through special meal requests, they contain indications of travellers' religious practices -- a category of information specially protected by many countries."
>
> (Edward Hasbrouck, "Total Travel Awareness")[213]

Secondly, as the Working Party noted:

> "... the issues at stake affect judicial and police co-operation and should be assessed in the light of the safeguards laid down in recent EU-US agreements and draft agreements concerning co-operation, mutual assistance and extradition."[214]

This means that, specifically, the EU-USA arrangements should not lead to evasion of the proper legal arrangements for the disclosure of evidence by police-, immigration- and law enforcement authorities and courts in EU Member States to their counterparts in the USA: international agreements on such matters provide for extensive safeguards, which should not be undermined.

This is the more so since, as the Working Party pointed out, thirdly:

> "The collection of the data included in the databases of airlines as requested by the US covers a large number of passengers (estimated to amount to at least 10-11 million per annum) which underlines the need for a cautious approach bearing in mind the possibilities this opens up for data mining affecting, in particular, European citizens and entailing the risk of generalised surveillance and controls by a third State."[215]

The Working Party therefore rightly concluded that "the requests coming from the US administration should be addressed with the utmost attention."[216] Indeed, the first and last of the above concerns apply equally to the intra-EU and global PNR proposals, while the second can be equated, in terms of intra-EU activity, to a concern about the effect of the dissemination of PNR data on EU Third Pillar activities generally. The EU-USA, the intra-EU, and the global proposals must all be treated with caution.

---

213 Full reference in footnote 43, above.

214 WP78, p. 5. Cf. the comment on p. 3 that "This opinion is given at a time when US are requesting from EU or directly from Member States numerous flows of personal data (e.g. visa, etc.)."

215 *Idem.*

216 *Idem.*

Another general issue is that, as the Working Party put it:

> "This is the first occasion in which the transfer takes place because of a legal obligation from a third country which requires operators in the EU to transfer data to a public authority in that third country in a way which is not in conformity with the Directive.
>
> In order to provide a sound legal basis for these transfers, a package is envisaged which consists of an adequacy decision and an international agreement, which is to accomplish a number of legal effects. The Working Party takes the view that, to the extent in which the International Agreement serves to legitimate a limitation of the right to private life, or a restriction of the purpose limitation principle in Article 6 of the Directive, it should in any case respect the limits of both Article 8 of the European Convention on Human Rights and Article 13 of the Directive."
>
> (WP87, p. 4)

This observations confirms the international human rights requirement that States may only demand that personal data be disclosed from the private sector to law enforcement- and anti-terrorist agencies if the demand:

(a) is based on law (in the sense of a clearly-defined and accessible legal rule);
(b) serves a specific, legitimate purpose in a democratic society;
(c) is strictly necessary and proportionate to the achievement of that purpose.[217]

The more specific remaining concerns about the transfer of PNR data to the USA (as expressed by the Working Party) relate, briefly, to the following:[218]

4.2.2 The purposes of the transfers; limits on further transfers

According to the US authorities, they will use the PNR data (only):

1. to prevent and combat terrorism and related crimes;
2. to prevent and combat other serious crimes of a transnational nature, including organised crime of that nature; and
3. to prevent and combat flight from US warrants or custody for such crimes.

(US undertakings of 12 January 2004)

The Working Party feels that the second category:

> "remains vague, in particular as for the scope of the 'other serious crimes' mentioned in the US Undertakings. Moreover, the purposes remain far broader than the focus on fighting acts of terrorism that the Working Party regarded as necessary in its opinion 4/2003."
>
> (WP87, p. 6)

---

[217] On the international-legal framework for privacy and law enforcement, see Paper No. 4.

[218] For full details, see Opinion 2/2004 in WP87. It is useful to compare the concerns discussed there with the earlier ones, set out in Opinion 4/2003 in WP78: although the Working Party sees progress, concerns remain on almost all issues identified in the earlier Opinion.

This concern is linked to a related one, about the possibility of further transfers of the PNR data to other US Government or foreign authorities:

> "The Working Party notes that a comprehensive list of the relevant government authorities to which data might be transferred has not yet been provided. The Working Party is also still concerned about such provisions allowing CBP to disclose data 'as otherwise required by law', especially if those provisions are considered in the light of existing or proposed laws and Memorandums of understanding requiring US to share their data with other countries in some specific cases.
>
> In particular, the mechanism referred to in points 29 and 35 of the Undertakings deviate considerably from the purpose limitation principle as stated by the Working Party (i.e. fight against terrorism and directly related crimes) and even from the wider purposes as defined in points 1 and 3 of the Undertakings."
>
> (WP87, pp. 9 – 10)

The Working Party is similarly concerned that the US undertaking with regard to the use of data "derived" from PNR data is too lax and may lead to breaches of the crucial purpose-limitation principle:

> "In additional wording for the Undertakings, the US authorities describe the limitations that exist to their accessing data 'derived' from PNR elements that may reveal features of a passenger's life and pose the risk of serious interference in the data subject's right to private and family life, under the terms of Article 8 of the European Convention on Human Rights. The new wording is as follows:
>
> > 'Additional personal information sought as a direct result of passenger PNR data will be obtained from sources outside the government only through lawful channels, and only for legitimate counter-terrorism or law enforcement purposes. For example, if a credit card number is listed in a PNR, transaction information linked to that account will be sought pursuant to lawful process, such as a subpoena issued by a grand jury or a court order, or as otherwise authorized by law. In addition, access to records related to e-mail accounts derived from a PNR will follow U.S. statutory requirements for subpoenas, court orders, warrants, and other processes as authorized by law, depending on the type of information being sought.'
>
> These clarifications are welcome. They do not, however, on their own fully allay the Working Party's concerns. In particular, the scope of the purposes for which PNR may be used should not allow for further unspecified 'law enforcement purposes'. Moreover, access to e-mail accounts and other personal information derived from a PNR should only take place in accordance with procedural requirements laid down in international instruments related to judicial and law enforcement cooperation. It must also be clear that in case of abuse, individuals can seek redress from an independent authority."
>
> (WP87, p. 8)

4.2.3 Limiting the amounts and kinds of personal data

Number of data fields

PNR records consist of between 5 and 60 data fields depending on the airline, including some that can specifically contain sensitive data (as defined below); some "open field"; and some

optional ones. In its Opinion 4/2003, the Working Party said that to transfer all the data in all these fields would go "well beyond what could be considered adequate, relevant and not excessive" - which means it would breach Art. 6(1)(c) of the Framework Directive. It suggested limiting the transfers to less than half this number, and excluding sensitive, open and optional fields.[219] But the US authorities still demand most of the data, without any evidence or explanation for this. The Working Party felt that any addition to its list of 19 fields should be subject "to a strict test" of proportionality and data-minimisation.[220]

Sensitive data

Article 8(1) of the Framework Directive places strict limitations on the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, or concerning health or sex life. The Working Party feels that no such "sensitive data" should be transferred. It did not believe that the US offer of elimination by means of "trigger words" would work and "invites the Commission to find the appropriate technical solutions (such as filters) in order to avoid any transmission of sensitive data to the US authorities."[221]

Biometric data

Elsewhere (in connection with its views that PNR data should not be used in CAPPS II or in the TIA effort, as separately discussed below) the Working Party stresses that the Commission should prohibit "any other further use of European passengers' data transmitted by airlines ... entailing the processing of biometric data."

4.2.4 Moment of transfers

The Working Party "regrets" that the authorities still demand access 72 hours before departure and the possibility of three updates, although it had suggested 48 hours with only one update.[222]

4.2.5 Retention period

The Working Party is unhappy with the retention period of 3½ years - which is much longer than the "weeks or months" it had suggested. It was also concerned about the 8-year retention period for any data actually accessed, and felt much stricter rules, on the Australian lines, should be adopted.[223]

4.2.6 Adopting a "push" method of transfer

---

219 WP78, p. 8: "Access to the full set of PNR data is excessive. Data should be limited to the following information : PNR record locator code, date of reservation, date(s) of intended travel, passenger name, other names on PNR, all travel itinerary, identifiers for free tickets, one-way tickets, ticketing field information, ATFQ (Automatic Ticket Fare Quote) data, ticket number, date of ticket issuance, no show history, number of bags, bag tag numbers, go show information, number of bags on each segment, voluntary/involuntary upgrades, historical changes to PNR data with regard to the aforementioned items."

220 WP87, p. 7.

221 *Idem*, pp, 7 – 8. in its earlier Opinion, it had said that only the "push" method of data transfer, discussed below, could achieve this.

222 *Idem*, p. 9

223 *Idem*, pp. 8 – 9.

In its latest Opinion on the January 2004 US undertakings, the Working Party recalls its Opinion 4/2003:

> "where it considered that the sole data transfer mechanism whose implementation does not raise major problems is the 'push' one – whereby the data are selected and transferred by airline companies to US authorities – rather than the 'pull' one – whereby US authorities have direct access to airline and reservation systems databases.
>
> The Working Party is seriously concerned that, even though US authorities have seen no objection for several months to the 'push' system, the appropriate technical mechanisms to implement a 'push' system operated directly by the European airlines are not yet in place. The Working Party considers that concrete measures should be adopted by April 2004 at the latest and urges the Commission to take immediate action with that aim. Furthermore, the Working Party underlines that no adequacy of the level of protection provided for by the US can be assumed without the establishment of a 'push' system."

In its earlier Opinion, the Working Party also noted that:

> "if a pull-system were implemented ... the entire Directive [EC Framework Directive on data protection] could be considered as being directly and completely appliable to the US authorities." (WP78, p. 7)

This is not repeated in the latest Opinion - although if anything, the passage quoted understates the position. There is no doubt that a "pull" system would mean that the Directive applies - or rather, that by virtue of Art. 4 of the Directive, the national data protection law of an EU Member State properly implementing the Directive *must* be applied to any such "pulling" of PNR data, and to any transfer and further use of such data in the USA, if the database from which the data were "pulled" is situated in the EU Member State concerned.[224]

[224] See D Korff, EU Laws on Data Protection, footnote 44, above, Chapter 2, section iv, *territorial scope*.

4.2.7 Data subject rights, enforcement and dispute settlement

The Working Party remains concerned about exemptions from data subject access, and about limitations to the right of access to data generated on the basis of PNR data, such as "risk profiles" and "exclusionary lists" (lists of persons who must be barred from boarding flights). It notes that the rights of non-US citizens to seek rectification of erroneous data are more limited than the rights of US citizens under the Freedom of Information Act. Being based only on the US undertakings, they also rest on less clear ground (as discussed under the next heading).

The Chief Privacy Officer of the Department of Homeland Security to whom complaints may be submitted is, moreover, not independent in the sense required by the EU Directive; there is no outside independent redress mechanism; and the US undertakings do not create rights for third parties (i.e. for data subjects).

The Working Party "welcomes" the US undertaking that an audit will be held of the system, at least once a year and "expects the reviews to be conducted with the necessary openness and transparency to be truly effective".[225] This is however by no means guaranteed: the undertaking merely allows Working Party to participate in the review as "experts" "assisting" the Commission; they have little formal status in the review. The review is furthermore basically limited to matters covered by the US Department of Homeland Security's Chief Privacy Officer's annual report: any matter not addressed in that report may only be examined in the EU-USA audit with the CPO's agreement.

4.2.8 The nature and level of the US commitments

In the Commission's usual "adequacy" findings, it is an important requirement that the third country in question ensures that data subjects are given enforceable rights against the body importing data from the EU. However, in connection with PNR transfers, and contrary to what the Working Party had demanded in its Opinion 4/2003:

> "... it is clear that the US undertakings will not be legally binding on the US side. Moreover, the newly added paragraph 47 at the end of the undertakings explicitly clarifies the legal enforceability of the US undertakings, stating that they 'do not create or confer any right or benefit on any person or party, private or public'.
>
> The Working Party therefore underlines that the level of commitments on the US side cannot be considered as meeting the requirements laid down in its Opinion 4/2003 and considers that this matter is an essential condition which should in any case be addressed before any arrangements are formalised."
>
> (WP87, pp. 5 – 6)

4.2.9 Data matching and data quality

In its latest Opinion, the Working Party notes the following new concern:

> "Recent experience showed that a new element has to be taken into consideration in addition to the concerns raised above. The passenger PNR data collected by CBP are

[225] WP87, p. 12.

> matched in US with lists of persons searched for. These processing operations led to the fact that several flights from EU had to be cancelled at the last minute. Information given publicly thereafter revealed that they where mistakes or cases of unclear or homonymy problems affecting data related to suspects of terrorism.
>
> These circumstances are related to the data protection principle of data quality. The Working Party considers that further initiatives should take place in order to prevent such consequences for passengers, crew members as well as airline companies."
>
> WP87, p. 12)

4.2.10 Excluding the use of PNR data for CAPPS-II and in TIA

Of particular interest to this paper is the final, strict limitation on the use of PNR data which the Working Party requires. This relates to the so-called "CAPPS-II" program and to the Information Awareness efforts described in section 3.

The CAPPS program is a system for the screening of airline passengers. The original CAPS program ("Computer Assisted Passenger Screening") was developed to allow airlines to avoid time-consuming "bag-matching" of passengers (a common security measure in Europe). This was subsequently developed and called CAPPS ("Computer Assisted Passenger *Pre*-Screening") or CAPPS-I. The system is described by Hasbrouck as follows:

> "Starting in 1998, the government began supplying the airlines with a secret CAPPS profiling algorithm, and all airlines based in the USA have been required to pass passenger data from their reservation systems through the system each time a passenger checks in. At first, CAPPS was applied only to passengers with checked luggage. Since 11 September 2001 CAPPS profiling has been extended to all airline passengers.
>
> If your reservation fits the CAPPS profile, you and your luggage are set aside for "secondary security screening" comparable to normal international screening. The airlines retain the reservation data (and, it appears, make it available to the government without requiring a warrant and without notifying travellers that the government is reviewing their travel histories), whether or not you fit the profile. Those who don't fit the profile, and their luggage, have otherwise been largely ignored. Even since 11 September 2001, passengers and luggage not selected by CAPPS for secondary screening are much less carefully checked than is the norm in most other countries."
>
> (Hasbrouck, "Total Travel information Awareness")

A new version of CAPPS, CAPPS-II, is under development. The precise technical details are not known, except that it is a system designed to "profile" airline passengers by reference to multiple sources, with the aim of rating each passenger according to the supposed risk he or she poses - with the basis for the assessment being hidden in a computer algorithm. Presumably, in line with the Information Awareness- and other programs described in section 3, the CAPPS-II programs is to be (or become) "intelligent" enough to create its own new algorithms on the basis of a "learning" process.[226] Some indeed claim that CAPPS-II and TIA are directly linked:

---

226 The ACLU calls CAPPS-II "a program built around a secret process for conducting background checks on every person who flies and rating them according to the risk that they supposedly pose to

> "CAPPS-II and the other current proposals don't appear likely to improve security, but seem intended much more for surveillance and monitoring: as a 'conveyor belt' to get travel data from the airlines into the military's 'Terrorism Information Awareness' (originally called 'Total Information Awareness') system, and as a mechanism for forcing travellers to identify themselves so that than travel records can be positively associated in government dossiers with particular individuals and with data about them from other sources."
>
> (Hasbrouck, "Total Travel Information Awareness")

According to the US authorities, CAPPS-II is not yet operational, and only used for "testing" (although, as we have seen with TIA, the line between the two does not appear to be a very strict one).

Whatever the claims about links between CAPPS-II and TIA, or about the operational status of CAPPS-II, the Working Party emphasised that it did not endorse any use of PNR data transferred from the EU in either program, operational or otherwise:

> "The Working Party expressly excluded the CAPPS II programme and any other system capable of performing mass data processing operations from the scope of its Opinion 4/2003.
>
> In fact, these systems are qualitatively different from the mere transfer of passenger PNR data and involve wide-ranging issues which should be clarified and specifically addressed by the Working Party, in consideration of the more pervasive effects that would affect the fundamental rights of the data subjects concerned.
>
> In particular, the CAPPS II system raises a number of peculiar issues that require not only specific consideration by the Working Party, but also different, higher safeguards. Any possible future decisions on CAPPS II would need specific consideration by the Working Party and should not automatically flow from an extension of the applicable scope of the Commission's first adequacy decision on the transfer of passenger PNR data to the US.
>
> Therefore, also in light of the circumstance that the Working Party has not been informed and consulted about the ultimate CAPSS II legal framework, any use of personal data by TSA with regard to the proposed CAPPS II system or its testing should be considered excluded now and in future from the applicable scope of the Commission's decision. In other words, the considerations made in this Opinion are based on the assumption that the Commission's decision will not be extended in future to CAPPS II, including indirect extension via the reference to internal US legislation; otherwise, far more critical remarks would have to be made already at this stage.
>
> **As a result, the Working Party recommends the Commission to make clear, through a specific clause in the decision, that US authorities shall refrain from using passenger PNR data transmitted from the EU not only to implement the CAPPS II system but also to test it.**

---

airline safety." ACLU Comments on Travel Privacy Report by European Groups, in: Transferring Privacy (footnote 43, above).

> **It is the Working Party's opinion that this should also apply to any other further use of European passengers' data transmitted by airlines in relation with other programmes such as Terrorism Information Awareness and US VISIT** ..."
>
> (WP87, p. 5, emphasis added)

4.3 Assessment

The Opinions of the Working Party - i.e. of the most authoritative governmental authorities in the EU on the issue of data protection - make clear that the undertakings by the US authorities on the obtaining, by them, of PNR data from the EU, and on the further uses of such data, are deficient in almost every respect:

- ✓ they allow for excessive amounts of data to be transferred;
- ✓ they do not provide sufficient safeguards against the transfer of sensitive data and do not contain an unambiguous prohibition on the use of such data in conjunction with biometric data;
- ✓ they require the data to be sent too far in advance of travel, to be updated too often, and to be retained for excessive periods (in particular on the mere basis that the data were "accessed", even if there was no indication of any criminal or even suspect matters);
- ✓ they do not provide for sufficient data protection rights; and
- ✓ they are lacking a truly independent supervisory and enforcement system.

Indeed, the undertakings are expressly stipulated to be not legally binding on the US side, and "do not create or confer any right or benefit on any person or party, private or public."

Most importantly, however, for this paper, is the fact that purpose-limitation is not sufficiently ensured, and that PNR data, or data generated on the basis of PNR data (such as "risk profiles") or derived from PNR data (e.g., through credit card- or email details found in PNR-fields) may well be "leaked" to other US agencies than the CBP, for other purposes than fighting terrorism, under vaguely-worded clauses referring to disclosures to other agencies "where required by [US] law" and to the use of the data for activities relating to "other serious crimes," - by-passing the safeguards and guarantees enshrined in international treaties on cross-border police- and judicial cooperation.

This applies in particular to CAPPS-II and TIA. The assurance given by the US authorities that PNR data will only be used in the "testing" of this system sound unconvincing in view of the fact that "prototype" systems related to the Information Awareness effort are already linked to operational activities. What is more, passenger data are clearly regarded by the US authorities as central to the Information Awareness effort. As Hasbrouck noted:

> "In the section of the report [on TIA to Congress] on 'Laws and Regulations Governing Federal Government Information Collection' (beginning on page 21), 'airline reservations' are the first and, in fact, the *only* specific category of data mentioned as potentially being scanned or monitored by TIA programs. But DARPA's own exhaustive list of laws and regulations potentially relevant to its operations, in the rest of that section

of the report, fails to find any that would restrict TIA access to airline reservations or other travel data.

At Senate hearings on TIA in May 2003, DARPA and DHS officials said TIA will avoid using privacy-sensitive medical or financial data, and will instead rely primarily on travel data (which Congress and the public are presumed to regard as less privacy-sensitive). According to a report of the hearing in the New York Times, DARPA's witness 'said the main area of private data that might be useful in anticipating terrorist attacks would be transportation records', and that TIA 'would rely mostly on information already held by the government, especially by law enforcement and intelligence agencies.'

It's hard to escape the conclusion that travel data is central to the government's current conception of TIA, that CAPPS-II may be **the** key data-acquisition mechanism for TIA, and that the use of data obtained through CAPPS-II has been the subject of specific TIA research and testing."

(Hasbrouck, "Total Travel Information Awareness", original emphases)

5. Conclusions

The demand for PNR data, and the CAPS-II and TIA programs must be seen as related, and probably (in the USA) as intended to be related. This should make for caution with regard to the proposed European and global PNR systems. The idea that State authorities should have unrestricted access to all the data in extremely large (and by their very size sensitive) private-sector databases, on millions of people, without any need to prove the relevance or necessity of access to data on any particular individuals, and that they should be allowed to carry out extensive "profiling" and "risk assessment" of entire populations, is anathema to the most fundamental principles of data protection and the rule of law. The use of PNR and other private- and public-sector data for such assessments is a highly significant step towards a surveillance society.

Specifically, we feel that the TIA program (as conceived) is the natural outcome of the trend we have discerned in the earlier (combined) papers. It represents the ultimate step in moves towards preventive, intelligence-led law enforcement. If the programs being developed under the TIA banner were to be shown to be effective in the fight against terrorism, there would be an unstoppable demand for their introduction in the fight against serious or organised crime (which is in any case inseparable from the fight against terrorism).

This is obvious for such programs as "next-generation face recognition" or computerised translation of texts in foreign languages. However, the same applies to the supposedly much more sophisticated pattern-recognition and -re-defining programs. If EELD could reliably classify a person as a "potential terrorist," it can surely also single out people who are likely to have committed a bank robbery or a rape, or some other heinous crime? Indeed, it would be useful if the system could predict who will rob banks, or will rape people...

However, as we hope to have shown, TIA-type programs have a long way to go to live up to this promise - and it is not clear that they ever will. Indeed, not only will they have an uncertain effect against terrorism or crime, they will have a more than just chilling effect on democratic freedoms. They could lead to the stigmatisation of minorities and ethnic, religious or cultural "out-groups" and can be used to harass political activists and others - with the basis for such stigmatisation and harassment hidden in impenetrable algorithms. Computer

screening of PNR data is likely to suffer from the same inherent defects, and to have the same negative effects. Indeed, political activists have already been "flagged" and prevented from travelling, without any serious evidence that they were involved in crime (let alone terrorism).

Our analysis of these matters thus shows that the European data protection authorities - and in the UK, the Information Commissioner - have a more important role to fulfil than previously realised. If ideas from the TIA program filter through into policing in Europe, and the UK, the Commissioner will have to work hard to maintain the view so clearly expressed by the Working Party that:

> "It is not proved that not taking into account properly the principles of proportionality and data minimization results into more efficiencies in combating terrorism and maintaining internal security, whilst respecting those principles constitutes an essential guarantee for safeguarding citizens' rights as well as being better suited for commercial development purposes. ... [T]he legitimate requirements of internal security and fight to terrorism can be pursued in a proportionate and reasonable way through systems which are in line with the fundamental principles of privacy and data protection."
>
> (WP87)

It is also clear, however, that in such a stand for fundamental rights and against ubiquitous surveillance, the odds are heavily loaded against him. As recent developments have shown, the claim that data protection merely serves to protect the guilty and that law-abiding citizens have nothing to fear from uninhibited data sharing and mining is forceful, even if untrue.

In the next paper, on the EU legal framework for privacy and law enforcement and on the national laws of a number of EU Member States, we will examine to what extent current EU- and national legal principles, and more in particular data protection principles, can be used in the defence of fundamental liberties threatened by the developments described in this paper. Some approaches, put forward by the Working Party, have already been noted, but will be revisited and elaborated on. Here, we may end by stressing that it will be crucial for the Commissioner to convince law enforcement and other agencies of the need for restraint and strict control, if they want to continue to police by consent rather than (information) power. But he will also need effective legal tools, and be willing to use those tools, for the protection of the most fundamental human freedoms under threat from the developments we have described.

- o – O – o –

DK
Cambridge/London, February 2004

fipr

Foundation for Information Policy Research

UK INFORMATION COMMISSIONER STUDY PROJECT:

PRIVACY & LAW ENFORCEMENT

Paper No. 4:

the legal framework

an analysis of the "constitutional" European approach
to issues of data protection and law enforcement

February 2004

CONTENTS

1. Introduction

This paper sets out the international/European and comparative legal framework for the processing of personal data for law enforcement purposes. The aim (as with the other papers) is to assist the Information Commissioner in the formulating of his general approach and specific policies in this area.

In the next section (section 2), the paper first places the UK Data Protection Act 1998 in its wider European-legal context (sub-section 2.1). Next, it addresses the nature and status of data protection in European law: it explains the complex nature of the concept, but also - with detailed reference to the case-law - how data protection is nonetheless subject to the standard, "constitutional"-legal approach to fundamental rights, developed by the European Court of Human Rights and also followed by the European Court of Justice (sub-section 2.2). In sub-section 2.3, we show how the Working Party established under the EC Framework Directive on data protection has adopted a similar, detailed approach to assessing the "adequacy" of data protection in third countries, which is again useful in pointing the way for similar assessments, to be made by the Information Commissioner in the UK.

In section 3, we will (after a brief discussion of the complex nature of the concept of "policing" in sub-section 3.1) discuss the approach to processing of personal data for law enforcement purposes in countries in which data protection has a constitutional bases (sub-section 3.2); and then (in sub-section 3.3) the leading European-level rules in the area.

A series of annexes provide basic reference material and further detail of the matters raised.

2. The European legal framework for data protection[227]

2.1 The Data Protection Act in its wider European-legal context

The UK Data Protection Act 1998 (hereafter: DPA98 or just "the Act")[228] gives effect to both the main Council of Europe treaty on data protection, the 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (hereafter: "the Council of Europe Convention," "the Data Protection Convention" or "Convention No. 108" after its number in the European Treaty Series, ETS)[229] and to the main (1995) EC directive on the matter, Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereafter: "the Framework Directive on data protection" or just "the Framework Directive").[230] As discussed below, at 2.2, these

---

[227] This section draws on (but also expands on and updates) sections in two reports prepared by the author for the European Commission in recent years, and in a forthcoming book: D. Korff, The feasibility of a seamless system of data protection rules for the European Union (Study Contract ETD/95/B5-3000/MI/169), Final Report, 1997 (published 1998), Part II, *The Directive*, section 1, *general: basic principles and criteria*, and Part IV, *The application of data protection in specific sectoral contexts*, section C, *the police sector*; D. Korff, Study on the protection of the rights and interests of legal persons with regard to the processing of personal data relating to such persons (Study Contract ETD/97/B5-9500/78), Final Report, 1998 (published 1999), section 2, *the international-legal framework for data protection*, and section 3, *the legislative situation in the Member States (and three non-Member States)*; D. Korff, Data Protection Law in the EU, 2004, Chapter 1, section iii, *aims and purposes: the [EC] Directives' "constitutional" status.*

[228] Data Protection Act 1998, 1998, c. 29.

[229] Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28 January 1981, ETS No. 108.

[230] Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, p. 31. In addition to the Framework Directive there are two subsidiary directives, which apply the principles of the Framework Directive in specific contexts: Directive 97/66/EC of the European Parliament and the Council of 4 November 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector (often referred to as "the ISDN Directive"), now defunct; and its successor, Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the

instruments in turn give effect to certain human rights enshrined in the European Convention on Human Rights ("ECHR"),[231] the principles of which also constitute "general principles of EC [and EU] law,"[232] and to certain rights set out in the Charter of Fundamental Rights of the European Union ("the Charter").[233]

Since 2000, the ECHR has been incorporated into UK law through the Human Rights Act (HRA), while EC law (and thus the Framework Directive) has supremacy over domestic UK law by virtue of the European Communities Acts 1972 and 1993, at least in matters within the scope of Community law. Indeed, as noted below, at 2.2, under the heading "case-law of the European Court of Justice," the basic principles and criteria set out in the Framework Directive are "directly applicable" and can be invoked by individuals in cases involving the processing of their personal data, in both the domestic courts and in the ECJ. The interpretation and application in practice of the DPA98 is therefore in crucial respects not simply a matter for the UK courts or for the Information Commissioner; rather, the Act must be seen as part of (and as embedded in) a wider international/European legal framework.[234]

This international/European legal framework is highly complex. However, as will also be shown below, at 2.2, certain important basic principles are clear. Moreover, in European law, and in many European national systems, these principles are seen as *constitutional* principles from which a State under the rule of law should not depart. Indeed, adoption of these broad principles is also in accordance with the new, "constitutional" approach to law, and to the rule of law, in the UK, as stressed most recently by no less an authority than the Lord Chief Justice, Lord Woolf.[235]

2.2 Data protection in European law

2.2.1 The complex nature of data protection as a fundamental right

There is considerable confusion about the nature, aim and scope of data protection. However, all the main international data protection instruments - the UN- and OECD Guidelines, the Council of Europe Convention and the EC Directives on data protection[236] - stress the link between data protection and the two "classical" human rights of respect for privacy or

---

processing of personal data and the protection of privacy in the electronic communications sector (directive on privacy and electronic communications or DPEC). The broad, "constitutional" matters relating to data protection (the basic data protection principles; the "criteria for lawful processing," and the rules governing exceptions and derogations) are addressed mainly in the Framework Directive - but equally apply to the way in which the subsidiary directives must be implemented. The discussion in this paper will therefore focus on the Framework Directive, with only occasional reference to the other directives.

231 European Convention for the Protection of Human Righs and Fundamental Freedoms, Rome, 4 November 1950, ETS No. 5.

232 See sub-section 2.2, below, about the status of the ECHR and data protection in the EC- and EU legal framework.

233 *Idem*. For the background to and text of the Charter, see the website of the Council or Consilium (the body which drafted it): http://db.consilium.eu.int/df/default.asp?lang=en. Note however that that website has not been kept up to date and only mentions the position at the Cologne and Tampere Councils of 1999, when the Consilium finished its work. In fact, the text of Charter was formally proclaimed by the Council of the EU, the European Parliament and the Commission in 2000: see the Conclusions of the Presidency of the Nice Council of December of that year at: http://db.consilium.eu.int/en/Info/eurocouncil/index.htm.

234 On the limited scope of the HRA compared to the ECHR, and on the limited scope of the EC directives (*qua* EC directives), see below, at 2.3 (where we conclude that these limitations should not affect the Information Commissioner's approach).

235 Cf. Lord Woolf, The Lord Chief Justice of England and Wales, The Rule of Law and a Change in the Constitution, Squire Centenary Lecture, Cambridge University, 3 March 2004. Lord Woolf focussed on the need for independent, judicial review of matters affecting the rights of citizens.

236 UN Guidelines for the regulation of computerized personal data files (E.CN.4/1990/72, adopted by the General Assembly on 20 November 1990, A/C.3/45/L.66); OECD Guidelines for the Protection of Privacy and Transborder Flows of Personal Data, contained in a Recommendation of the Council of the OECD, adopted on 23 September 1980 (hereafter "the OECD Guidelines"). The discussion in this paper is limited to the European instruments and –principles. Suffice it to note that these principles are equally reflected in (although perhaps not always as fully developed in) wider international law.

"private life" and freedom of expression (while remaining rather unclear about the precise nature of this link).

As far as the first of these fundamental rights is concerned, the EC Framework Directive on data protection thus stipulates that:

> "In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data." (Art. 1(1) of the Framework Directive)

This is reiterated, in similar terms, in the same paragraphs of the same article of the other two (subsidiary) directives (see Art. 1(1) of the Telecommunications Data Protection Directive and Art. 1(1) DPEC).

Moreover, the Framework Directive (and by extension the other data protection directives) expressly seeks to "give substance to and amplify" the data protection principles set out in Council of Europe Convention No. 108 (see Preamble (11) to the Framework Directive), which Convention in turn seeks to "secure" the right to privacy (or "private life") as contained in Art. 8 of the European Convention on Human Rights (Art. 1 of the Convention No. 108).

The fundamental rights and freedoms enshrined in the European Convention on Human Rights (including Art. 8) are, in turn, granted quasi-constitutional status in the EC (and the EU) as "general principles of Community law." As it is put in Art. 6 of the Treaty on European Union:

> "The Union shall respect fundamental rights, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms signed in Rome on 4 November 1950 and as they result from the constitutional traditions common to the Member States, as general principles of Community law."[237]

In other words, the UK Data Protection Act gives effect to an EC data protection directive which builds on the Council of Europe Data Protection Convention in order to secure to individuals the protection of Art. 8 of the European Convention on Human Rights, and compliance with "general principles of European Community [and Union-] law,"[238] with respect to the processing of personal data.

Ultimately, the European courts (the European Court of Human Rights in Strasbourg and the European Court of Justice in Luxembourg) can be called upon to rule on whether the Act, or the interpetration or application of the Act in practice, meets the requirements of this provision and these principles. We will discuss below what this entails, with reference to the case-law of these judicial bodies.

Before doing so we should note, however, that the legal situation is in fact even more complicated. Thus, first of all, since "data" is broadly speaking just another word for

---

[237] Formerly Art. F.2. On the political-legal background to the recognition of human rights norms as "general principles of Community law", see D Korff, Human Rights in the European Union, Bilbao, 1994. Cf. also: Affirming fundamental rights in the European Union: Time to act, Report of the Expert Group on Fundamental Rights established by the European Commission (then DG XV), 1999.

[238] On the status of the ECHR as general principles, not just of European Community-, but of European Union law, see the discussion of the EU Charter and the Constitution, below.

"information" (or is at least included in the latter concept),[239] data protection also touches on the freedom to seek, receive and impart information, which is also guaranteed by the European Convention on Human Rights, in Art. 10. The Explanatory Memorandum to the Council of Europe Convention on Data Protection thus expressly notes that:

> "certain rights of the individual may have to be protected vis-à-vis the free flow of information regardless of frontiers, the latter principle being enshrined in international and European instruments on human rights (see Article 10 European Human Rights Convention; Article 19 International Covenant on Civil and Political Rights). Where the present convention imposes certain restrictions or conditions on the exercise of freedom of information, it does so only to the extent strictly justified for the protection of other individual rights and freedoms, in particular the right to respect for individual privacy (see Article 8, European Convention [on Human Rights])."
>
> (Explanatory Memorandum to the Council of Europe Convention on data protection, para. 19)

The same can be said of the EC data protection directives, and of the national laws giving effect to the directives, including the DPA98: they too limit the internationally guaranteed right to seek, receive and impart information without interference by public authority and regardless of frontiers, in order to protect the equally internationally guaranteed right to privacy and protection of private life.

However, data protection is not fully caught by either Art. 8 or Art. 10 ECHR, or indeed by both of them together, but relates to wider issues and other rights protected the European Convention on Human Rights. Data protection is therefore increasingly recognised as a new right of its own, *sui generis*.

2.2.2 Data protection as a new right *sui generis*

Hondius (in a way the "intellectual father" of the Council of Europe Convention on data protection) observed almost 20 years ago (with reference to events 30 years ago) that one could not expect adequate data protection to be developed solely from case-law on the above-mentioned provisions of the ECHR:

> "We consider the right to privacy, as formulated in Article 8 of [the European Convention on Human Rights] hardly fit for such new case-law even with Westin's added dimension of 'information privacy'. It simply does not correspond to the reality of data processing. Article 10, freedom of information is not very suited either because data protection deals both with access to and limitations on access to information. Article 8 and 10 are each other's reflection in the mirror, each having a second paragraph enabling them to undo undesirable effects of the application of the main rule. For the citizens and the data users it seems unsatisfactory to construct data protection by a complicated juggling act between two counterbalancing articles and their restrictions."[240]

---

239 The words are used more or less as synonyms in the EC Framework Directive and the other data protection directives. The UK DAP98 makes a distinction, in that it applies the term "data" to certain categories of information only (the categories of data falling within the scope of the EC Framework Directive, plus an additional category of information in separately defined "accessible records") - but the distinction does not lead to significant discrepancies between the Act and the Framework Directive.

240 Frits W Hondius, A decade of international data protection, in: *Netherlands International Law Review*, Vol. XXX (1983), p. 103ff, at 127.

Indeed, several aspects of data protection relate to Convention rights and other "general principles of law" *other* than the right to private life and freedom of expression and information. Specifically, under Articles 6 and 13 of the Convention and Article 1 of the First Protocol to the Convention, and under various general principles of law, people should have an opportunity to find out what information, held on them by other persons, is used to take "significant decisions" on them; and they should be able to challenge the accuracy, up-to-dateness and relevance of the data in those contexts. The collecting, storing and (in particular) the use of information on the religious, political or other opinions on persons, and the processing of information on their group affiliations of this kind, furthermore affects the rights to freedom of thought, conscience and religion (Article 9), the right to freedom of expression (Article 10), the right to freedom of association (Article 11), and the right not to be discriminated against on such grounds (Article 14).

The Explanatory Report to the Council of Europe Convention thus acknowledges that:

> "**The unfettered exercise of the freedom to process information may, under certain conditions, adversely affect the enjoyment of other fundamental rights (for example privacy, non-discrimination, fair trial) or other legitimate personal interests (for example employment, consumer credit)**."
>
> (Explanatory Memorandum, para. 25, with reference to the Preamble to the Convention).[241]

That data protection has a broader aim then just to protect privacy or "private life" is also clear from the core data protection principles, common to all the international and most national data protection instruments (cf. Art. 5 of the Council of Europe Convention; Art. 6 of the Framework Directive): Many of the principles can be linked to the need to protect privacy, and to prevent undue interference with the "private life" of individuals, e.g. the principle that personal data should only be collected if there is a good reason to do so (for a "specified" and "legitimate" purpose), or the principle that only such data should be collected as are relevant to such an end. However, the requirement that data should be "adequate" for the purpose in question[242] already points to a wider aim: it implies a duty of persons or companies or authorities which use personal data to act with due diligence, to ensure that they have all the relevant information available, and base their decisions only on such relevant information. The data subject rights are equally aimed, not just at ensuring that intrusive and unwarranted data gathering or –storage can be stopped, but also to allow for the correction of erroneous data, to ensure that all appropriate information - and only the appropriate information - is taken into account in making decisions which affect the interests of data subjects.

---

[241] The Explanatory Memorandum to the OECD Guidelines makes the same point: "*The remedies under discussion are principally safeguards for the individual which will prevent an invasion of privacy in the classical sense, i.e. abuse or disclosure of intimate personal data; but other, more or less closely related needs for protection have become apparent. Obligations of record-keepers to inform the general public about activities concerned with the processing of data, and rights of data subjects to have data relating to them supplemented or amended, are two random examples. Generally speaking, there has been a tendency to broaden the traditional concept of privacy ('the right to be left alone') and to identity* ***a more complex synthesis of interests which can perhaps more correctly be termed privacy and individual liberties***." (Explanatory Memorandum to the OECD Guidelines, para. 2, emphasis added). The other instruments show a similar ambiguity, by referring to the need to reconcile freedom of information with privacy "*in particular*", or "*notably*" with privacy, or with "*values such as*" privacy. Such references too confirm that more is at stake than just the "privacy" or "private life" of individuals.

[242] The OECD Guidelines say that the data must be "complete".

The fact that data protection was increasingly seen as a *sui generis* right, related to but distinct from Articles 8 and 10 ECHR, was one of the main reasons for giving it protection separate from those articles. Initially, consideration was given to the drawing up of a further Additional Protocol to the European Convention on Human Rights, adding data protection to the catalogue of rights in the Convention as a new, independent right. In the end, the Council of Europe decided to draw up a separate treaty, the Data Protection Convention (Convention No. 108), mainly because the Human Rights Convention is open only to Member States of the Council of Europe, whereas a separate convention could be drafted in such a way as to allow non-European States too to become a party.[243]

One implication of this wider scope of data protection (as compared to privacy or "private life") is that it may need to be extended, even by reference to the ECHR and the EC/EU "general principles of law" to "legal persons," such as companies or associations. Thus, the European Court of Human Rights has been reluctant to apply Article 8 ECHR to legal persons (although it did extend the right to privacy to law offices), but has extended the other rights just mentioned (Articles 6 and 13, Article 1 First Protocol, Articles 9, 10, 11 and 14) to groups, associations, companies etc., to various degrees. The subsidiary data protection directives and several national laws also expressly extend some data protection guarantees to legal persons.[244] This again emphasises the special, *sui generis* nature of the concept.

The Charter of Fundamental Rights of the European Union, already mentioned,[245] takes the same view: while the right to privacy or "private life" is guaranteed by Art. 7[246] (and freedom to seek, receive and impart information by Art. 11), the Charter guarantees data protection for citizens of the Union in a separate article:[247]

> *Article 8*
> **Protection of personal data**
>
> 1. Everyone has the right to the protection of personal data concerning him or her.
>
> 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
>
> 3. Compliance with these rules shall be subject to control by an independent authority.

---

243 Hondius, footnote 13 above, pp. 126 – 127. See also para. 19 of the Explanatory Memorandum to the Data Protection Convention.

244 For a full discussion of the issue, see D. Korff, Study on the protection of the rights and interests of legal persons with regard to the processing of personal data relating to such persons, *o.c.* (above, footnote 1).

245 See footnote 7, above.

246 Article 7 of the Charter simply reads: "*Everyone has the right to respect for his or her private and family life, home and communications.*" This follows the text of the ECHR, except that the word "correspondence" in the Convention has been replaced by the work "communications," to underline that the right applies to all forms of communications, including telephone-, fax- and email communications.

247 Note that, as far as the application of data protection within the Communities is concerned, the Intergovernmental Conference inserted, through the Amsterdam Treaty, a new provision in the EC Treaty requiring adherence by the institutions to the rules of the Data Protection Directive and the monitoring of this adherence by an independent supervisory body (Art. 286 ECT). A regulation to give effect to this commitment was adopted at the end of 2000: Regulation (EC) No.45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.

If the EU Constitution is adopted as planned, it will incorporate the Charter, and thus this provision, in Part II of that instrument.[248]

2.2.3 The "constitutional" approach to data protection

Irrespective of whether one sees data protection as a right flowing (in particular) from the right to "private life" in Art. 8 ECHR, or as a new *sui generis* right, one matter is clear: from the European-legal perspective at least, it is to be regarded as a fundamental right. In many EU Member States, too, the matter is emphatically regarded as a constitutional issue (even if the exact constitutional basis for data protection can differ between those States).[249]

This status of data protection as an international-legally guaranteed, "constitutional" issue has important implications for the manner in which the specific rules in the relevant instruments are applied. The European Court of Human Rights in particular has developed a clearly-defined, systematic approach to such issues, which builds on the structure of the most important rights in the ECHR, including, significantly, both Art. 8 and Art. 10. In cases touching on such matters, the European Court of Justice follows this same approach.

We will examine the specific case-law of these courts on data protection issues in more details, below. Here, we may first set out this **standard, typical, "constitutional" approach** in general terms.[250]

2.2.4 The standard approach of the European Court of Human Rights to cases under Arts. 8-11 of the European Convention on Human Rights

Articles 8 – 11 ECHR are all identically structured: they first set out (in their first paragraph) the right which must be guaranteed, and they then set out the permissible exceptions to the right concerned (in their second paragraph). Thus, Art. 8 ECHR reads:

> *Article 8*
> **Right to respect for private and family life**
>
> 1. Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

---

[248] For the text of the Draft Treaty establishing a Constitution for Europe as published (in 24 languages) on 18 July 2003, see: http://european-convention.eu.int/bienvenue.asp?lang=EN. Under this draft, the provision on data protection within the institutions, mentioned in the previous footnote, now Art. 286 ECT, will be included in the general Union principles in Part I of the Constitution if that instrument is adopted as drafted (see Art. I-50 of the Draft Constitution).

[249] For details of the different national-legal views, see D. Korff, Study on the protection of the rights and interests of legal persons with regard to the processing of personal data relating to such persons, *o.c.* (above, footnote 1), Section 3.1; D. Korff, Data Protection law in the EU, *o.c.* (*idem*), Annex 3, *Comparative Report*, section 1, *constitutional status of data protection*.

[250] The "constitutional" status of the ECHR has been stressed by the Court itself, which has said that it reflects a "European *ordre public*. It is also clear from the fact that, nowadays, membership of the Council of Europe - which is open only to democracies which respect the rules of law - is contingent on accession to the Convention. The same is true of the recognition of the requirements of the Convention as "general principles" of EC- and EU law by the ECJ. The outline of the standard approach (indented in the text) is taken from a teaching handout by the author. For a very simple introduction into the approach to these matters, see D Korff, The guarantee of freedom of expression under Article 10 of the European Convention on Human Rights, in *Media Law & Practice*, Vol. 9, Nr. 4 (December 1988), p. 143ff. Further detail (with extensive reference to the case-law) can be found in Harris, O'Boyle & Warbrick, Law of the European Convention on Human Rights, London, Dublin, Edinburgh, 1995, p. 285ff.

4. The Legal Framework

The European Court of Human Rights has developed a standard approach to cases under these articles. It always follows this approach in cases under these articles. In fact, its line of thinking is so ingrained that the most important elements can very often also be noted in cases under other articles of the Convention, even if those are not structured in the same way as Arts. 8-11 (e.g. in cases concerning the right to property, Art. 1 First Protocol; or even with regard to elements of Art. 2, concerning the right to life).

Very broadly, the Court examines the following issues, in the following order:

1. Did the matter complained of (the alleged violation of the Convention) fall within the ambit of the right concerned, e.g. for an Art. 10 case: did the matter complained of concern the exercise, by the applicant, of his or her right to freedom of expression?

If the matter did not fall within the ambit of the right there can of course also be no violation of the right (NB if the matter does not fall within the ambit of any of the substantive provisions of the Convention, the case is declared "inadmissible *ratione materiae*").

2. Was there a restriction or limitation placed on the exercise of the right?

If not, there was no violation.

3. Was the restriction imposed by a public authority?

If not, there is usually no violation because the Convention has no "horizontal effect." However, sometimes a State can be held responsible for not taking measures to prevent interferences with the exercise of the right by private parties (so-called "indirect horizontal effect").

4. Was the restriction in accordance with or authorised by "law"?

If not, then that in itself means that there was a violation - irrespective of whether the measure was reasonable or even necessary. The term "law" is given an "autonomous" meaning: it includes not just statutes but also subsidiary rules and regulations and indeed judge-made (common) law - but in order for a rule to qualify as "law", the rule must be accessible (i.e. published or at least available) and sufficiently clear to be "foreseeable" in its effect: individuals must be able to know what they are or are not allowed to do.

5. Did the restriction serve one of the "legitimate interests" listed in the article concerned, e.g. public safety, morals etc.? (Note: this equates to the question of whether there was a "pressing social need")

If it does not, there is a violation (but it is extremely rare for the Court to find this).

6. Was the restriction "necessary in a democratic society" to protect the legitimate interest concerned?

This is mainly a question of *proportionality*: if the legitimate interest in question (say, public security) could have been protected by means of less severe restrictions than the one imposed, the restriction was disproportionate and thus not "necessary".

However, it is in this respect that the State is granted a "*margin of appreciation*": the Court feels that the State is in a better position to judge what is "necessary" to serve certain interests, but this goes "hand in hand with European supervision".

In practice, the application of the "necessity" test and the width of the "margin of appreciation" depend on a range of factors, such as the nature of the right (thus, freedom of expression is regarded as of fundamental importance in a democratic society and interferences with this right are thus in principle subject to strict scrutiny by the Court, while other rights may be given less weight); the objectivity of the "legitimate interest" pursued (which means that the Court grants States a wider margin with regard to morals than for say health); or whether there is a European consensus (if so, there is a narrower margin: it is difficult to argue that a restriction on something is "necessary" in one European country if it is not considered necessary anywhere else in Europe). Other international instruments and sources can also be important, e.g. a special treaty on the issue (such as Convention No. 108 on data protection), or a Recommendation adopted by the Committee of Ministers of the Council of Europe (such as Recommendation R(87)15 Regulating the Use of Personal Data in the Police Sector): the existence of such instruments, especially if widely adopted, points to a broad European consensus and thus implies that the State has only a narrow margin of appreciation.

The Council of Europe Convention on data protection (Convention No. 108) and the EC Framework Directive on data protection (Directive 95/46/EC) both adopt the same approach, except that they set out the permissible restrictions, which in the Human Rights Convention are set out, for the crucial provisions, Arts. 8 - 11, in the second paragraphs of those provisions, in one general exception clause, modelled on those second paragraphs of those Convention articles.

The relevant article in Convention No. 108 reads as follows:

Article 9
Exceptions and restrictions

1 No exception to the provisions of Articles 5, 6 and 8 of this convention shall be allowed except within the limits defined in this article.

2 Derogation from the provisions of Articles 5, 6 and 8 of this convention shall be allowed when such derogation is provided for by the law of the Party and constitutes a necessary measure in a democratic society in the interests of:

a protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences;

b protecting the data subject or the rights and freedoms of others.

3. ... [251]

The exception clause in the Framework is very similar; it reads:

Article 13
[**Exemptions and restrictions**][252]

1. Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6 (1), 10, 11 (1), 12 and 21 when such a restriction constitutes a necessary measure to safeguard:

(a) national security;

(b) defence;

(c) public security;

(d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;

(e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;

(f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);

(g) the protection of the data subject or of the rights and freedoms of others.

2. ... [253]

The phrases "*provided for by law*" and "*necessary measure in a democratic society*," as used in Art. 9 of Convention No. 108, as well as the words "*legislative measure[s]*" and "*necessary*" as used in Art. 13 of the Framework Directive, must be given the same meaning,

---

[251] Art. 9(3) contains an additional exception concerning the use of statistical data. It reads: "*Restrictions on the exercise of the rights specified in Article 8, paragraphs b, c and d, may be provided by law with respect to automated personal data files used for statistics or for scientific research purposes when there is obviously no risk of an infringement of the privacy of the data subjects.*"

[252] The title ("exemptions and restrictions") is taken from the heading to Section VI of the Framework Directive: Art. 13 is the only article in this section.

[253] Art. 13(2), like Art. 9(3) of the Council of Europe Convention, noted in the previous footnote, contains an additional exception concerning the use of statistical data. It reads: "*Subject to adequate legal safeguards, in particular that the data are not used for taking measures or decisions regarding any particular individual, Member States may, where there is clearly no risk of breaching the privacy of the data subject, restrict by a legislative measure the rights provided for in Article 12 when data are processed solely for purposes of scientific research or are kept in personal form for a period which does not exceed the period necessary for the sole purpose of creating statistics.*"

and must be applied in the same way, as the corresponding terms in the second paragraphs of Arts. 8 – 11 of the Human Rights Convention. **In other words, the "standard approach" to these Convention articles, set out above, also applies to the data protection instruments, and in particular to any processing which departs from the basic data protection principles, such as disclosing public- or private-sector data to the police for law enforcement purposes; non-informing of data subjects of such disclosures; denial of access to data in police files; etc..** The very same "check-list" must be followed - and is followed in the cases of the European courts relating to data protection issues, discussed later.

Here, it may be noted that the first point on the "check-list" - whether an issue falls within the ambit of the relevant provision of the ECHR - may, for data protection matters, often be subsumed under the more precise questions of whether the matter in question: (a) concerned "personal data"; (b) involved "processing" of such data; and (c), with regard to non-automated data, whether those data were held in the relevant kind of (structured) "personal data filing systems." In order to answer those questions, the terms used must be clarified, and we will come to that later. Here, it may suffice to note that **if a particular action involves automated processing of personal data, or non-automated processing of personal data in structured filing systems, the matter must be assessed by reference to the criteria listed, from the second point onwards.**

In addition, under the ECHR, great emphasis is placed on **remedies** and **safeguards**, and on **procedure**. This applies in general, but also especially as concerns secret measures (such as the interception or monitoring of communications, or video- or audio surveillance) impinging on protected rights.

On the basic right to a remedy, the ECHR stipulates the following:

Article 13
Right to an effective remedy

> Everyone whose rights and freedoms as set forth in this Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity.

The Court has held that this right must be granted, not just to everyone whose rights have been proven to have been violated (which would rob the provision of independent meaning), but to anyone with an "arguable claim" to that effect.[254]

In addition, the existence of **effective procedural safeguards** surrounding the imposition of measures interfering with fundamental rights (such as telephone- or mail interceptions) is a crucial matter to be taken into account in the assessment of the "necessity" of an interference, especially as concerns secret police and intelligence activities. To some extent, the issues of safeguards, remedies and procedures overlap: the absence of sufficient safeguards will undermine the effectiveness of available remedies. In the view of the Court, secret measures which would normally violate Convention rights (such as telephone interception or the keeping of secret files) may become acceptable if they are subject to adequate supervision and safeguards: subject to such safeguards they may be "necessary in a democratic society" to

[254] Silver v the UK. Note that Art. 13 ECHR is not included in the HRA. This has been criticised by human rights organisations such as *Liberty* and *Justice*.

counter crime or to protect national security, whereas without them, they would not be "necessary" in such a society.[255]

The European data protection instruments again reflect this position and if anything give such matters additional emphasis, by making elaborate provision for remedies, procedures and safeguards (even if the precise nature of such safeguards is often still left open). Here, it may suffice to list the range of safeguards which the Framework Directive on data protection requires the EU Member States to provide (with references in footnotes to more detailed discussions of these matters):

(a) Transparency about the processing of personal data generally[256]

See Arts. 18, 19 and 21 of the Framework Directive, concerning notification (registration) of processing operations and publication of the notified details (and of the same details of operations which are exempt from notification). Note also the special requirement of "prior checking" for sensitive operations, stipulated in Art. 20: this special, stricter requirement is a typical reflection of the principle of "proportionality" which, as we have seen, is closely linked to the test of "necessity" to be applied under the Human Rights Convention and EU law.

(b) Duties to inform data subjects of relevant matters[257]

See Arts. 10 and 11 of the Framework Directive, concerning, respectively, the information that has to be provided to the data subjects when data are collected from them, and the information that must be provided to them when data on them are collected otherwise. Note in particular the stipulation that the Member States must require that more than basic information must be provided whenever this is necessary to ensure "fairness" *viz-à-viz* the data subject: this too reflects the principles of "proportionality" and "necessity:" if the additional information is not provided, the processing is "unfair" and unlawful.

(c) Data subject rights[258]

See Arts. 12, 14 and 15 of the Framework Directive. Article 12 concerns the right to obtain confirmation of processing of data on the data subject, and details of such processing, on request; the right of access to these data; the right to obtain the rectification, erasure or blocking of incorrect data or data which are processed in contravention of the laws implementing the Directive; and the right to have third parties to whom the data were disclosed informed of such corrections or deletions. Article 14 concerns the general right to object to processing "on justified grounds" and the special (absolute) right to object to the processing of one's data for direct marketing purposes. And Art. 15 gives data subjects the right "*not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him*," i.e. to decisions based on computer-generated "personality profiles."[259]

---

255 Cf. the *Klass*- and *Leander*-cases, discussed below. Note that this means that the absence of the "right to a remedy" from the HRA can perhaps, to some extent, be remedied by reference to the "necessity" test, also in relation to the processing of personal data: see section 4, *Conclusions*, below.

256 For a full discussion, see D. Korff, Data Protection law in the EU, *o.c.* (footnote 1, above), Chapter 7.

257 *Idem*, Chapter 4.

258 *Idem*, Chapter 5.

259 This rather difficult provision has particular relevance for the use of computer-generated algorithms in the fight against terrorism, discussed in Paper No. 3. We will return to this in the Final Paper.

(d) Remedies to be granted to data subjects[260]

Data subjects must be granted a range of remedies: the right to complain to the national data protection authority (Art. 28(4) of the Framework Directive); the right to a judicial remedy against any breaches of their rights, both separate from complaints to the data protection authority and on appeal from the latter's determination of or handling of such complaints (Art. 22); and the right to obtain compensation for any damages suffered as a result of processing contrary to the national law implementing the Directive (Art. 23).

(e) Sanctions against wrongful processing[261]

In addition to remedies that data subjects may use, the State must also provide for its own, autonomous sanctions against controllers in the public and private sector which process personal data in contravention of the law (Art. 24 of the Framework Directive). While the Directive as such is silent on the nature of these sanctions, they typically include both administrative sanctions and orders, and criminal penalties.

(f) Additional, special safeguards relating to processing on the basis of exceptions to or derogations from the normal data protection rules and principles

The Framework Directive contains a number of provisions which allow for departures from certain basic provisions in special cases. Thus, Art. 6(1)(b) in effect allows for departures from the strict application of the "purpose-limitation" principle, for the benefit of historical, statistical or scientific research purposes. Article 8(4) authorises less clearly defined departures from the in-principle prohibition on the processing of "sensitive data," for reasons of "substantial public interest." Crucially, however, the Directive adds that, in such cases Member States must, in the law authorising such departures from the basic rules, provide "appropriate-" or "suitable safeguards," over and above the other safeguards and remedies listed here. Some Member States have not yet fully provided for such safeguard. However, others have laid down such safeguards, by stipulating, e.g., with regard to the use of data for research purposes, that such data must as far as possible be anonymised or pseudonymised, and/or that such processing must be authorised by a special body or council; or with regard to processing for reasons of "substantial public interest," that the basic rule authorising such processing must be contained in a formal law (a Statute), further regulated in precise, detailed, published regulations, and subject to close supervision and review.[262]

(g) General supervision by data protection authorities[263]

Finally, the Framework Directive demands that Member States appoint an independent "supervisory authority" (or several such authorities)(Art. 28). The supervisory authority must be given a range of functions, including monitoring the operation of the national data protection law and advising the Government on "administrative measures or regulations" relating to data protection (Art. 28(1) and (2)). More importantly for the present purpose, under Art. 28(3), the authority must be endowed with:

---

260 See D. Korff, Data Protection law in the EU, *o.c.* (footnote 1, above), Chapter 6, section *iv*.

261 *Idem*, Chapter 6 and (on the different types of sanctions provided for in the laws of the Member States) Annex 3, *Comparative Summary*, section 13, remedies, liability and sanctions.

262 *Idem*, Annex 3, *Comparative Summary*, section 5.3, safeguards for scientific processing.

263 *Idem*, Chapter 6, in particular section *i*,

- **investigative powers** - including powers of access to data and other relevant information;

- **enforcement powers** ("effective powers of intervention") - including the power to order the blocking, erasure or destruction of data, to impose a temporary or definitive ban on processing, or to warn or admonish a controller; as well as the power to issue "opinions" on processing operations subject to a "prior check" and to publish such opinions;

- **powers of referral** - including both the power to refer relevant matters to Parliament or other political institutions and the power to bring suspected violations of the law to the attention of the courts or the prosecuting authorities.

The authorities must also, as already noted, be able to receive complaints ("claims") from data subjects (Art. 28(4)). Here, it may be added that in this respect they must be able, "in particular, [to] hear claims for checks on the lawfulness of data processing lodged by any person when the national provisions adopted pursuant to Article 13 of this Directive [that is: the exceptions to the national law relating to such matters as law enforcement and national security] apply." The national data protection authorities must also publish a regular (typically annual) report (Art. 28(5)); and they must give each other information, as well as assistance in transnational cases (Art. 28(6)).

In the UK, the designated "supervisory authority" is, of course, the Information Commissioner.

The point to be made here about these safeguards, remedies, procedures and authorities is that they are part of the "constitutional" approach to data protection. Failure to provide the required basic safeguards will, in terms of the Human Rights Convention, normally mean that the processing contravenes Art. 8, or that the individuals concerned (the data subjects) are denied an effective remedy, in violation of Art. 13, or both.

If, in exceptional cases, the normal, basic safeguards are disapplied, or a remedy (or access to a remedy) is denied, or if the processing is not subject to the normal supervisory mechanisms - then alternative safeguards, alternative remedies have to be put in place. In assessing the compatibility of such special rules with the "constitutional" requirements, the need for any departure from the normal rules and the strength and effectiveness of the alternative safeguards must be assessed. Only exceptional circumstances can justify a departure from basic data protection rules and –principles; and the further exceptional rules depart from the normal ones, the more stringent and effective should the special supervisory mechanisms be. Applying such yardsticks - rather than uncritical deference to statutory or executive attempts to modify the operation of the normal rules whenever this is deemed convenient - is what the "constitutional" approach to data protection entails.

This is well illustrated by the case-law of both the European Court of Human Rights and the European Court of Justice, to which we now turn.

2.2.5 Case-law of the European Commission and Court of Human Rights[264]

[264] The European Commission of Human Rights has been abolished by the 11th Protocol to the Convention, but is referred to here in relation to the early case-law. Otherwise, the summary is limited to the case-law of the Court.

4. The Legal Framework

Partly because of the rather uneasy link between data protection and the rights currently enshrined in the ECHR, discussed above, the case-law under the Convention relating to the processing of personal information has developed only slowly. Mostly, it is based on Art. 8 of the Convention: the European Court of Human Rights has consistently refused to build any measure of data protection on Article 10 of the Convention, which (as was noted above) guarantees *inter alia* "freedom to receive and impart information". As the Court put it, bluntly, in the Leander- and Gaskin-judgments, discussed below:

> "The Court observes that the right to freedom to receive information basically prohibits a Government from restricting a person from receiving information that others wish or may be willing to impart to him. **Article 10 does not**, in circumstances such as those of the present case, **confer on the individual a right of access to a register containing information on his personal position, nor does it embody an obligation on the Government to impart such information to the individual.**"
>
> (Leander-judgment, para. 74, emphasis added; expressly confirmed in para. 52 of the Gaskin-judgment).

As far as Art. 8 ECHR is concerned, it should first be noted that the term "privacy" is not used in that article. Rather, it stipulates in its first paragraph that:

> "Everyone has the right to respect for his private and family life, his home and his correspondence."

Article 8 therefore protects a range of interests. Data protection relates to only one of these: "private life", but the latter term also encompasses other matters. On the protection of that right, Harris, O'Boyle and Warbrick observed:

> "The Commission's practice concerning the meaning of private life has been distinguished neither by its clarity nor its discipline. The Commission has not been careful to distinguish the ambit of private life from the content of the state's obligation to respect private life. Nor has it kept separate the questions whether a state has failed to respect private life in breach of Article 8(1) and whether an interference with a right is justified under Article 8(2).
>
> Similarly, the Court in the Niemitz v Germany case was unwilling to attempt an exhaustive definition of private life, or even to isolate the values it protects. However, the Court did give some guidance as to the meaning or ambit of 'private life' for the purposes of Article 8 and other aspects of it emerge from the jurisprudence of both the Commission and the Court. In Niemitz, the Court said:
>
> > '... it would be too restrictive to limit the notion [of private life] to an 'inner circle' in which the individual may live his own personal life as he chooses and to exclude therefrom entirely the outside world not encompassed within that circle. Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings.'
>
> The Court thus endorsed a long practice of the [European Commission of Human Rights] in which it had sought to extend the concept of private life beyond the

> narrower confines of the Anglo-American idea of privacy, with its emphasis on the secrecy of personal information and seclusion."[265]

The Commission and Court of Human Rights have consequently included a range of more specific interests within the scope of the concept of "private life": freedom of individuals (including prisoners) to associate with others; freedom to engage in sexual activities; the physical and moral integrity of the person (including protection from sexual assault and corporal punishment); and indeed protection of the human "identity" (in particular in transsexual cases). These interests are inherently limited to natural person only. However, in the case of Niemitz, the Court held that some personal relations in a business context could fall within the scope of "private life".

Like most of the other substantive provisions of the Convention, Article 8 is subject to an exception clause, contained in the second paragraph of the article. As explained above, this paragraph prohibits states from "interfering" with the exercise of the rights protected by the first paragraph unless the interference is "in accordance with law" and "necessary in a democratic society" for the protection of certain important public interests (national security, public safety, the prevention of crime or disorder, the protection of health or morals), or for the protection of the rights or freedoms of others.

The Court has also consistently held that telephone calls received on private or business premises are covered by the notions of "private life" and "correspondence" within the meaning of Article 8(1);[266] and that the interception and recording of such calls by law enforcement or other State agencies constitutes an "interference by a public authority" with those rights.[267] The Court has not, to date, been specifically asked to rule on the question of whether monitoring of communications without access to the contents of such communications - as in the "metering" of telephone calls - constitutes an interference with the interests protected by Art. 8, but we submit is should be regarded as such, because of the detailed insight into a person's "private life" which it allows. The reference in the Kopp-judgment, quoted in the passage from the Amann-judgment set out below, to "tapping *and other forms of interception* of telephone conversations" suggests that such a wider reading is appropriate.

Here, it may suffice to note the importance which the Court attaches to the "quality" of any law regulating such matters, and to the importance of appropriate safeguards against "arbitrary" use of powers of secret surveillance. To use the Court's own summary of its approach, in the Amann-judgment further discussed below:

> "*Quality of the law*
>
> The Court reiterates that the phrase 'in accordance with the law' implies conditions which go beyond the existence of a legal basis in domestic law and requires that the legal basis be 'accessible' and 'foreseeable'.
>
> According to the Court's established case-law, a rule is 'foreseeable' if it is formulated with sufficient precision to enable any individual – if need be with appropriate advice – to

---

265 Harris, O'Boyle & Warbrick, Law of the European Convention on Human Rights, 1995, pp. 305 – 306, footnote references omitted.

266 See the Halford v. the United Kingdom judgment of 25 June 1997, para. 44.

267 see the *Kopp v. Switzerland* judgment of 25 March 1998, para. 53.

regulate his conduct (see the Malone v. the United Kingdom judgment of 2 August 1984, Series A no. 82, pp. 31-32, § 66). With regard to secret surveillance measures the Court has underlined the importance of that concept in the following terms (ibid., pp. 32-33, §§ 67-68):

> "The Court would reiterate its opinion that the phrase 'in accordance with the law' does not merely refer back to domestic law but also relates to the quality of the law, requiring it to be compatible with the rule of law, which is expressly mentioned in the preamble to the Convention ... The phrase thus implies – and this follows from the object and purpose of Article 8 – that there must be a measure of legal protection in domestic law against arbitrary interferences by public authorities with the rights safeguarded by paragraph 1 ... Especially where a power of the executive is exercised in secret, the risks of arbitrariness are evident...
>
> ... Since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the legal discretion granted to the executive to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference."

It has also stated that 'tapping and other forms of interception of telephone conversations constitute a serious interference with private life and correspondence and must accordingly be based on a 'law' that is particularly precise. It is essential to have clear, detailed rules on the subject, especially as the technology available for use is continually becoming more sophisticated' (see the Kopp judgment cited above, pp. 542-43, § 72)."

(Amann-judgment, paras. 55 – 56)

Article 8 also covers the use of CCTV camera surveillance - another matter which is of relevance to the present study. The most authoritative case in this regard is the recent case of Peck v. the United Kingdom.[268] The case concerned the use of a CCTV system operated by UK local council, covering a public road, and the release of footage of the applicant to the press.

The applicant had been depressed at the time, and had attempted to cut his wrists with a knife, unaware that this was noted by the CCTV operators. The latter notified the police, who came to the scene. They took the knife from the applicant, gave him medical assistance and brought him to the police station. He was detained under the Mental Health Act 1983, but released without charge and taken home by police officers after having been treated by a doctor. The council released still photographs from a video of CCTV footage of the applicant in its own publication, "CCTV News", and gave copies of the photographs and the video to the media, as part of a campaign by the council to demonstrate the benefits of its CCTV system. These did not show the actual suicide attempt, but did show the applicant with the knife. Stills from the video were published in a local paper, and parts of the video itself were used in television reports. The face of the applicant had not, or not adequately, been masked; the authorities had not sought his permission for the release of the footage.

The Court's assessment of whether the actions of the authorities constitute an "interference" with the applicant's rights under Art. 8 of the Convention usefully recalls earlier relevant rulings, and links the issues in Peck with those in the cases of Amann and Rotaru, discussed below, and deserves to be set out here in full:

---

[268] Judgment of 28 January 2003.

"*The Court's assessment*

Private life is a broad term not susceptible to exhaustive definition. The Court has already held that elements such as gender identification, name, sexual orientation and sexual life are important elements of the personal sphere protected by Article 8. The Article also protects a right to identity and personal development, and the right to establish and develop relationships with other human beings and the outside world and it may include activities of a professional or business nature. There is, therefore, a zone of interaction of a person with others, even in a public context, which may fall within the scope of 'private life' (*P.G. and J.H. v. the United Kingdom*, no. 44787/98, § 56, ECHR 2001-IX, with further references).

In the above-cited *P.G. and J.H.* case the Court further noted as follows (paragraph 57):

> "There are a number of elements relevant to a consideration of whether a person's private life is concerned in measures effected outside a person's home or private premises. Since there are occasions when people knowingly or intentionally involve themselves in activities which are or may be recorded or reported in a public manner, a person's reasonable expectations as to privacy may be a significant, though not necessarily conclusive factor. A person who walks down the street will, inevitably, be visible to any member of the public who is also present. Monitoring by technological means of the same public scene (e.g. a security guard viewing through close circuit television) is of a similar character. Private life considerations may arise however once any systematic or permanent record comes into existence of such material from the public domain."

The monitoring of the actions of an individual in a public place by the use of photographic equipment which does not record the visual data does not, as such, give rise to an interference with the individual's private life (see, for example, *Herbecq and Another v. Belgium*, applications nos. 32200/96 and 32201/96, Commission decision of 14 January 1998, DR 92-A, p. 92). On the other hand, the recording of the data and the systematic or permanent nature of the record may give rise to such considerations. Accordingly, in both the *Rotaru* and *Amann* judgments (to which the *P.G. and J.H.* judgment referred) the compilation of data by security services on particular individuals even without the use of covert surveillance methods constituted an interference with the applicants' private lives (*Rotaru v. Romania* [GC], no. 28341/95, §§ 43-44, ECHR 2000-V, and *Amann v. Switzerland* [GC], no. 27798/95, §§ 65-67, ECHR 2000-II). While the permanent recording of the voices of *P.G.* and *J.H.* was made while they answered questions in police cell as police officers listened to them, the recording of their voices for further analysis was regarded as the processing of personal data about them amounting to an interference with their right to respect for their private lives (the above-cited *P.G. and J.H.* judgment, at §§ 59-60).

However, the Court notes that the present applicant did not complain that the collection of data through the CCTV camera monitoring of his movements and the creation of a permanent record of itself amounted to an interference with his private life. Indeed, he admitted that that function of the CCTV system together with the consequent involvement of the police may have saved his life. Rather he argued that it was the disclosure of that record of his movements to the public in a manner in which he could never have foreseen which gave rise to such an interference.

In this respect, the Court recalls the Lupker and Friedl cases decided by the Commission which concerned the unforeseen use by the authorities of photographs which had been previously voluntarily submitted to them (*Lupker and Others v. the Netherlands*, no. 18395/91, Commission decision of 7 December 1992, unreported) and the use of

photographs taken by the authorities during a public demonstration (*Friedl v. Austria*, judgment of 31 January 1995, Series A no. 305-B, Friendly Settlement, Commission report of 19 May 1994, §§ 49-52). In those cases, the Commission attached importance to whether the photographs amounted to an intrusion into the applicant's privacy (as, for instance, by entering and taking photographs in a person's home), whether the photograph related to private or public matters and whether the material thus obtained was envisaged for a limited use or was likely to be made available to the general public. In the *Friedl* case, the Commission noted that there was no such intrusion into the 'inner circle' of the applicant's private life, that the photographs taken of a public demonstration related to a public event and that they had been used solely as an aid to policing the demonstration on the relevant day. In this context, the Commission attached weight to the fact that the photographs taken remained anonymous in that no names were noted down, the personal data recorded and photographs taken were not entered into a data processing system and no action had been taken to identify the persons photographed on that occasion by means of data processing (see *Friedl v. Austria*, the above cited Commission report, §§ 50-51). Similarly, in the *Lupker* case, the Commission specifically noted that the police used the photographs to identify offenders in criminal proceedings only and that there was no suggestion that the photographs had been made available to the general public or would be used for any other purpose.

The present applicant was in a public street but he was not there for the purposes of participating in any public event and he was not a public figure. It was late at night, he was deeply perturbed and in a state of some distress. While he was walking in public wielding a knife, he was not later charged with any offence. The actual suicide attempt was neither recorded nor therefore disclosed. However, footage of the immediate aftermath was recorded and disclosed by the Council directly to the public in its 'CCTV News'. In addition, the footage was disclosed to the media for further broadcast and publication purposes. Those media included the audio-visual media: Anglia Television broadcast locally to approximately 350,000 people and the BBC broadcast nationally and it is 'commonly acknowledged that the audio-visual media have often a much more immediate and powerful effect than the print media' (*Jersild v. Denmark*, judgment of 23 September 1994, Series A no. 298, § 31). The 'Yellow Advertiser' circulated in the applicant's locality to approximately 24,000 persons. The applicant's identity was not adequately, or in some cases not at all, masked in the photographs and footage so published and broadcast. He was recognised by certain members of his family and by his friends, neighbours and colleagues.

As a result, the relevant moment was viewed to an extent which far exceeded any exposure to a passer-by or to security observation (as in the above-cited *Herbecq* case) and to a degree surpassing that which the applicant could possibly have foreseen when he walked in Brentwood on 20 August 1995.

Accordingly, the Court considers that the disclosure by the Council of the relevant footage constituted a serious interference with the applicant's right to respect for his private life."

(paras. 57 – 63)

The Court accepted that the capture and use of the footage was "in accordance with law" (*in casu*, section 163 of the Criminal Justice and Public Order Act 1994 and section 111 of the Local Government Act 1972, both of which, the Court said, "complied with the Convention's 'quality of law' requirements") (paras. 66 – 67). It also served "legitimate aims", i.e. public safety, the prevention of disorder and crime and the protection of the rights of others (in that

the Court accepted that trying to make a CCTV system more effective through advertising it and its benefits served those aims) (para. 67 and 79).

The crucial question was whether the interference was "necessary in a democratic society". After discussing other earlier case-law,[269] the Court carefully weighed the different elements of the case and the conflicting interests involved, with particular reference to alternative actions which had been available to the authorities:

> "As to the present case, the Court would note at the outset that the applicant was not charged with, much less convicted of, an offence. The present case does not therefore concern disclosure of footage of the commission of a crime.
>
> The Court has also noted, on the one hand, the nature and seriousness of the interference with the applicant's private life (paragraph 63 above). On the other hand, the Court appreciates the strong interest of the State in detecting and preventing crime. It is not disputed that the CCTV system plays an important role in these respects and that that role is rendered more effective and successful through advertising the CCTV system and its benefits.
>
> However, the Court notes that the Council had other options available to it to allow it to achieve the same objectives. In the first place, it could have identified the applicant through enquiries with the police and thereby obtained his consent prior to disclosure. Alternatively, the Council could have masked the relevant images itself. A further alternative would have been to take the utmost care in ensuring that the media, to which the disclosure was made, masked those images. The Court notes that the Council did not explore the first and second options and considers that the steps taken by the Council in respect of the third were inadequate."
>
> (paras. 79 – 80)

After further, detailed consideration of these alternatives, the Court concludes:

> "In sum, the Court does not find that, in the circumstances of this case, there were relevant or sufficient reasons which would justify the direct disclosure by the Council to the public of stills from the footage in own publication 'CCTV News' without the Council obtaining the applicant's consent or masking his identity, or which would justify its disclosures to the media without the Council taking steps to ensure so far as possible that such masking would be effected by the media. The crime prevention objective and context of the disclosures demanded particular scrutiny and care in these respects in the present case.
>
> ...
>
> Accordingly, the Court considers that the disclosures by the Council of the CCTV material in the 'CCTV News' and to the 'Yellow Advertiser', Anglia Television and to the BBC were not accompanied by sufficient safeguards to prevent disclosure inconsistent with the guarantees of respect for the applicant' private life contained in Article 8 of the Convention. As such, the disclosure constituted a disproportionate and

[269] This included the case of Z. v Finland, judgment of 25 February 1997, which concerned the disclosure in court proceedings without the applicant's consent of his health records including his HIV status. The Court found that that disclosure had violated Z's rights under Art. 8. It may be noted that the Court, in Peck, expressly recalled its reference to the Data Protection Convention in the case of Z: see the Peck-judgment, para. 78.

> therefore unjustified interference with his private life and a violation of Article 8 of the Convention."
>
> (paras. 85 and 87)[270]

Most important for the present paper, however, is the application of the concept of "private life" to the collecting, storing and use of personal information, and to the rights of the individuals concerned in this respect. This is an area in which the case-law has developed slowly. Thus, in an early case, X v Federal Republic of Germany (1973),[271] the Commission held that the collecting and storing of information by the police did not, as such, conflict with Article 8 - even when (as in that case) the data subject had no criminal record. The main consideration appears to have been that the information had not been disclosed by the police to anyone. In a case six years later, the Commission considered the dissemination of police data to a criminal court justified in the interest of the prevention of crime, but expressly left open the question of whether this processing raised an issue under the first paragraph.[272]

The processing of personal data was examined more searchingly in two subsequent cases. The Leander case[273] concerned a secret police register, which contained information on the applicant. On the basis of this secret information, he was denied a job at a museum situated on the territory of a Swedish naval base. He had been denied access to the file and had no opportunity to refute the information used against him. In this case, the Court ruled, for the first time, that such registering of personal information could, as such, interfere with "private life" (although it still qualified this by stressing the absence of a possibility to challenge the data):

> "It is uncontested that the secret police-register contained information relating to Mr. Leander's private life.
>
> Both the storing and the release of such information, which were coupled with a refusal to allow Mr. Leander an opportunity to refute it, amounted to an interference with his right to respect for private life as guaranteed by Article 8 § 1." (para. 48 of the judgment)

In assessing whether the interference was justified in terms of the second paragraph of Article 8, the Court held that,

> "... in view of the risk that a system of secret surveillance for the protection of national security poses of undermining or even destroying democracy on the ground of defending it, the Court must be satisfied that there exist **adequate and effective guarantees against abuse**." (para. 60, emphasis added)

---

270 Para. 86 (omitted from the quote, above) refers to the fact that the applicant had himself appeared in the media after the release of the footage. The Government has argued that this stopped him from complaining about the original release, but the Court dismissed this: "*the Court does not find that the applicant's later voluntary media appearances diminish the serious nature of the interference or reduce the correlative requirement of care concerning disclosures. The applicant was the victim of a serious interference with his right to privacy involving national and local media coverage: it cannot therefore be held that against him that he sought thereafter to avail himself of the media to expose and complain about that wrongdoing.*"

271 Appl. No. 5877/72, YB XVI (1973), p. 328, at 388.

272 Appl. No. 8170/78, X v Austria, YB XXIII (1979), p. 308, at 320-322.

273 Leander v Sweden, judgment of 26 March 1987, A-116.

In the end, the Court held that in the special circumstances of the case (a security check required to protect national security), the special safeguards were sufficient: there had therefore been no violation of Article 8.[274]

The next leading case on access to personal information held in files is the case of Gaskin v the United Kingdom.[275] Mr Gaskin had been brought up in the care of local authorities and alleged that he had been ill-treated. He sought access to his file "to obtain details of where he was kept and by whom and in what conditions in order to be able to help him overcome his problems and learn about his past." Under English law at the time, such access was always denied unless the people who had written the relevant file documents expressly consented to their notes being disclosed. The Court ruled as follows:

> "In the Court's opinion, persons in the situation of the applicant have a vital interest, protected by the Convention, in receiving the information necessary to know and to understand their childhood and early development. On the other hand, it must be borne in mind that confidentiality of public records is of importance for receiving objective and reliable information, and that such confidentiality can also be necessary for the protection of third persons. Under the latter aspect, a system like the British one, which makes access to records dependent on the consent of the contributor, can in principle be considered to be compatible with the obligations under Article 8, taking into account the State's margin of appreciation. The Court considers, however, that under such a system the interests of the individual seeking access to records relating to his private and family life must be secured when a contributor to the records either is not available or improperly refuses consent. Such a system is only in conformity with the principle of proportionality if it provides that an independent authority finally decides whether the access has to be granted in cases where a contributor fails to answer or withholds consent. No such procedure was available to the applicant in the present case.
>
> Accordingly, the procedures followed failed to secure respect for Mr Gaskin's private and family life as required by Article 8 of the Convention. There has therefore been a breach of that provision." (paragraph 49 of the judgment)

Although still hedged about with ambiguity, the Leander- and Gaskin-judgments did move the case-law further into the direction of holding that the collecting, storing and use of personal information *ipso facto* constitute "interferences" with the right to "private life", which must be based on "law" and justified as "necessary in a democratic society" for the protection of other, *in casu* overriding public or private interests. As Harris, O'Boyle and Warbrick put it, with reference to further case-law:

> "The collection of information by officials of the state about an individual without his consent will interfere with his right to respect for his private life."[276]

---

274 There is an interesting footnote to this case, in that the Swedish Government subsequently admitted that its claims in the case were untrue, and that the file on Mr Leander "turned out to be a gossipy and mistake-filled assemblage of harmless information". See the article "*EU rights law* [sic] *rests on Swedish lies*, Guardian, 30 December 1997.

275 Judgment of 7 July 1989, A-160.

276 Harris, O'Boyle & Warbrick, o.c. (*supra*, footnote 38), p. 309.

The Court confirmed this in the case of Amann v. Switzerland.[277] The case concerned the interception of telephone calls from the embassy of the USSR (as it was at the time) to a Swiss businessman, about the sale of a depilatory device, and the creation of a card on the businessman, held in the Public Prosecutor's national security card index. The person calling the businessman was under surveillance, the businessman was (according to the Government) "fortuitously" caught by this surveillance (para. 61).

The Court examined the possible legal bases for this surveillance (about which there was disagreement) in some detail. It concluded that two provisions which had been invoked by the Government lacked the required quality and safeguards, because they contained:

> "no indication as to the persons concerned by such measures, the circumstances in which they may be ordered, the means to be employed or the procedures to be observed. That rule cannot therefore be considered to be sufficiently clear and detailed to afford appropriate protection against interference by the authorities with the applicant's right to respect for his private life and correspondence."
>
> (para. 58; cf. also para. 59)

With regard to other statutory provisions, in the Federal Criminal Procedure Code, the Court held:

> "[The main provision] defines the categories of persons in respect of whom telephone tapping may be judicially ordered and the circumstances in which such surveillance may be ordered. Furthermore, [certain subsequent provisions] set out the procedure to be followed; thus, implementation of the measure is limited in time and subject to the control of an independent judge, in the instant case the President of the Indictment Division of the Federal Court.
>
> The Court does not in any way minimise the importance of those guarantees. It points out, however, that the Government were unable to establish that the conditions of application of [the main provision] had been complied with or that the safeguards provided for in [the other provisions] had been observed.
>
> ...
>
> The primary object of the Federal Criminal Procedure Act is the surveillance of persons suspected or accused of a crime or major offence (...), or even third parties presumed to be receiving information from or sending it to such persons (...), but the Act does not regulate in detail the case of persons monitored 'fortuitously' as 'necessary participants' in a telephone conversation recorded by the authorities pursuant to those provisions. In particular, the Act does not specify the precautions which should be taken with regard to those persons.
>
> The Court concludes that the interference cannot therefore be considered to have been 'in accordance with the law' since Swiss law does not indicate with sufficient clarity the scope and conditions of exercise of the authorities' discretionary power in the area under consideration.

277 Judgment of 16 February 2000.

It follows that there has been a violation of Article 8 of the Convention arising from the recording of the telephone call received by the applicant on 12 October 1981 from a person at the former Soviet embassy in Berne."

(paras. 60 – 62).

As far as the creation of a card on the applicant was concerned, it is worth quoting the judgment at some length, as it well illustrates the "constitutional" approach to the matter. Also particularly notable is the express reference to the Council of Europe Convention on data protection: this emphasises the close link between that Convention and the ECHR.

"II. ALLEGED VIOLATION OF ARTICLE 8 OF THE CONVENTION ARISING FROM THE CREATION OF A CARD AND THE STORING THEREOF IN THE CONFEDERATION'S CARD INDEX

The applicant complained that the creation of a card on him, following the interception of a telephone call he had received from a person at the former Soviet embassy in Berne, and the storing thereof in the Confederation's card index had resulted in a violation of Article 8 of the Convention.

A. Applicability of Article 8

The Court reiterates that the storing of data relating to the 'private life' of an individual falls within the application of Article 8 § 1 (see the Leander v. Sweden judgment of 26 March 1987, Series A no. 116, p. 22, § 48).

It points out in this connection that the term 'private life' must not be interpreted restrictively. In particular, respect for private life comprises the right to establish and develop relationships with other human beings; furthermore, there is no reason of principle to justify excluding activities of a professional or business nature from the notion of "private life" (see the Niemietz v. Germany judgment of 16 December 1992, Series A no. 251-B, pp. 33-34, § 29, and the Halford judgment cited above, pp. 1015-16, § 42).

That broad interpretation corresponds with that of the Council of Europe's Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data, which came into force on 1 October 1985 and whose purpose is 'to secure in the territory of each Party for every individual ... respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him' (Article 1), such personal data being defined as 'any information relating to an identified or identifiable individual' (Article 2).

In the present case the Court notes that a card was filled in on the applicant on which it was stated that he was a 'contact with the Russian embassy' and did 'business of various kinds with the [A.] company' (...).

The Court finds that those details undeniably amounted to data relating to the applicant's 'private life' and that, accordingly, Article 8 is applicable to this complaint also.

B. Compliance with Article 8

1. Whether there was any interference

The Government submitted that the issue whether there had been 'interference' within the meaning of Article 8 of the Convention remained open since 'the card contained no

> sensitive information about the applicant's private life', the latter 'had not in any way been inconvenienced as a result of the creation and storing of his card' and that it had 'in all probability never been consulted by a third party'.
>
> The Court reiterates that the storing by a public authority of information relating to an individual's private life amounts to an interference within the meaning of Article 8. The subsequent use of the stored information has no bearing on that finding (see, *mutatis mutandis*, the Leander judgment cited above, p. 22, § 48, and the Kopp judgment cited above, p. 540, § 53).
>
> In the instant case the Court notes that a card containing data relating to the applicant's private life was filled in by the Public Prosecutor's Office and stored in the Confederation's card index. In that connection it points out that it is not for the Court to speculate as to whether the information gathered on the applicant was sensitive or not or as to whether the applicant had been inconvenienced in any way. It is sufficient for it to find that data relating to the private life of an individual were stored by a public authority to conclude that, in the instant case, the creation and storing of the impugned card amounted to an interference, within the meaning of Article8, with the applicant's right to respect for his private life."
>
> (paras. 64 – 70)

On the question of whether the interference was based on "law", the Court distinguished between the creation of the card and its subsequent retention in the index.

On the first point, the Court noted that none of the relevant provisions, invoked by the Government as possible legal basis for the creation of the card, expressly mentioned the existence of a register kept by the Public Prosecutor's Office. This:

> "raises the question whether there was 'a legal basis in Swiss law' for the creation of the card in question and, if so, whether that legal basis was 'accessible' (see the Leander judgment cited above, p. 23, § 51). It observes in that connection that [the relevant instructions] were above all intended for the staff of the federal administration."
>
> (para. 75)

The Court did not find it necessary to give a formal ruling on this, however, "*since even supposing that there was an accessible legal basis for the creation of the card in December 1981, that basis was not 'foreseeable'*" because it was based on the same provisions as the ones which authorised the telephone surveillance, and which the Court had already found to lack the "quality" to be considered "law" in the Convention sense (as noted above) (para. 76).

The Court went on to consider a set of specific Federal data protection regulations:

> "As regards the Federal Council's Directives of 16 March 1981 applicable to the Processing of Personal Data in the Federal Administration, they set out some general principles, for example that 'there must be a legal basis for the processing of personal data' (section 411) or that 'personal data may be processed only for very specific purposes' (section 412), but do not contain any appropriate indication as to the scope and conditions of exercise of the power conferred on the Public Prosecutor's Office to gather, record and store information; thus, they do not specify the conditions in which cards may

> be created, the procedures that have to be followed, the information which may be stored or comments which might be forbidden.
>
> Those directives, like the Federal Criminal Procedure Act and the Federal Council's Decree of 29 April 1958 on the Police Service of the Federal Public Prosecutor's Office, cannot therefore be considered sufficiently clear and detailed to guarantee adequate protection against interference by the authorities with the applicant's right to respect for his private life.
>
> The creation of the card on the applicant was not therefore 'in accordance with the law' within the meaning of Article 8 of the Convention."
>
> (paras. 76 – 77)

On the storing of the card in the Federal national security index, the Court first pointed out that "*it would seem unlikely that the storing of a card which had not been created 'in accordance with the law' could satisfy that requirement.*" (para. 78). In addition, the Court found that "Swiss law, both before and after 1990, expressly provided that data which turned out not to be "necessary" or "had no further purpose" should be destroyed - but that "*[i]n the instant case the authorities did not destroy the stored information when it emerged that no offence was being prepared, as the Federal Court found in its judgment of 14 September 1994.*" (*idem*). It concluded that the storing of the card on the applicant, too, was not "in accordance with the law" within the meaning of Article 8 of the Convention (para. 79).

The applicant also claimed that he had been denied an "effective remedy" against the violations of the Convention (Art. 13 ECHR), but does not appear to have pursued this matter very vigorously. The Court held that he did have such a remedy since "*the applicant was able to consult his card as soon as he asked to do so, in 1990, when the general public became aware of the existence of the card index being kept by the Public Prosecutor's Office*"; he had been able to lodge an administrative-law action in the Federal Court both about the lack of a legal basis for the telephone tapping and the creation of his card and about the lack of an "effective remedy" against those measures; and the Federal Court had jurisdiction to rule on those complaints and duly examined them (see paras. 85 – 90). However, the Court did not examine whether Mr. Amann had been denied an "effective remedy" prior to 1990, when he (like the rest of the Swiss population) had been unaware of the existence, not just of a card on him, but of the Federal national security card index system altogether.

The final case to be mentioned in this brief overview of the case-law is the case of Rotaru v. Romania. The case concerned the retention, retrieval and use, by the current Romanian Intelligence Service (*Serviciul Român de Informa□ i* – "the RIS"), of a file on the applicant created by the immediate post-WWII State security services, which, when they were disbanded in 1949, had forwarded it to the *Securitate* (the State Security Department of the Communist State), which had in its turn forwarded it to the RIS in 1990. The contents of the file became known through a letter sent by the Ministry of the Interior to a court hearing a case brought by the applicant alleging that he had been persecuted by the Communist regime. The files were clearly inaccurate: they listed the applicant as a university student when he was still at school, and mentioned a different faculty from the one he subsequently joined, and wrongly classified him as a member of an extreme right-wing organisation.

The Court first addressed certain preliminary matters of interest to this study, with reference to earlier case-law:

> "The Court reiterates, as to the concept of victim, that an individual may, under certain conditions, claim to be the victim of a violation occasioned by the mere existence of secret measures or of legislation permitting secret measures, without having to allege that such measures were in fact applied to him (see the Klass and Others v. Germany judgment of 6 September 1978, Series A no. 28, pp. 18-19, § 34). Furthermore, "a decision or measure favourable to the applicant is not in principle sufficient to deprive him of his status as a 'victim' unless the national authorities have acknowledged, either expressly or in substance, and then afforded redress for, the breach of the Convention" (see the Amuur v. France judgment of 25 June 1996, *Reports of Judgments and Decisions* 1996-III, p. 846, § 36, and *Dalban v. Romania* [GC], no. 28114/95, § 44, ECHR 1999-VI)."
>
> (para. 35)

The next question concerned the applicability of Art. 8 ECHR, i.e. the question of whether the issue fell within the ambit of that article:

> "The Government denied that Article 8 was applicable, arguing that the information in the RIS's letter of 19 December 1990 related not to the applicant's private life but to his public life. By deciding to engage in political activities and have pamphlets published, the applicant had implicitly waived his right to the 'anonymity' inherent in private life. As to his questioning by the police and his criminal record, they were public information.
>
> The Court reiterates that the storing of information relating to an individual's private life in a secret register and the release of such information come within the scope of Article 8 § 1 (see the Leander v. Sweden judgment of 26 March 1987, Series A no. 116, p. 22, § 48).
>
> Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings: furthermore, there is no reason of principle to justify excluding activities of a professional or business nature from the notion of 'private life' (see the Niemietz v. Germany judgment of 16 December 1992, Series A no. 251-B, pp. 33-34, § 29, and the Halford v. the United Kingdom judgment of 25 June 1997, *Reports* 1997-III, pp. 1015-16, §§ 42-46).
>
> The Court has already emphasised the correspondence of this broad interpretation with that of the Council of Europe's Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data, which came into force on 1 October 1985 and whose purpose is 'to secure ... for every individual ... respect for his rights and fundamental freedoms, and in particular his right to privacy with regard to automatic processing of personal data relating to him' (Article 1), such personal data being defined in Article 2 as 'any information relating to an identified or identifiable individual' (see *Amann v. Switzerland* [GC], no. 27798/95, § 65, ECHR 2000-II).
> Moreover, public information can fall within the scope of private life where it is systematically collected and stored in files held by the authorities. That is all the truer where such information concerns a person's distant past.
>
> In the instant case the Court notes that the RIS's letter of 19 December 1990 contained various pieces of information about the applicant's life, in particular his studies, his political activities and his criminal record, some of which had been gathered more than fifty years earlier. In the Court's opinion, such information, when systematically collected and stored in a file held by agents of the State, falls within the scope of 'private life' for

> the purposes of Article 8 § 1 of the Convention. That is all the more so in the instant case as some of the information has been declared false and is likely to injure the applicant's reputation.
>
> Article 8 consequently applies."
>
> (paras. 42 – 44)

The above passage should be important to the Information Commissioner, because it touches on the question of what constitutes "**personal data**". We are aware of the fact that that issue is the subject of another study commissioned by the Commissioner, but feel we should at least briefly mention our views, based on the European case-law, in view of the explicitly narrow interpretation given to the term by the UK Court of Appeal in the case of Durant v FSA (8 December 2003, Case No: B2/2002/2636).[278] We submit that the above judgment - and for that matter, the judgment of the ECJ in the Linqvist case mentioned by the Court of Appeal and discussed under the next heading - shows that, since data protection is a constitutional matter, the term should be given a *wide* meaning. Rather than data protection having to be narrowly applied to matters deemed to be strictly "private" (as the Court of Appeal suggests), the European Court of Human Rights goes the other way: it extends the concept of "private life" to fit in with the new, *wider* concept of data protection. As the Court puts it: its recent case-law "*emphasise[s] the correspondence of this **broad** interpretation [of Art. 8 of the Human Rights Convention] with that of the [Data Protection Convention]*."[279]

We might add that the Court of Appeal's narrow interpretation also starkly contrasts with the broad interpretation given to the concept of "personal data" in the other EU Member States.[280]

We believe that the approach of the Court of Appeal runs counter to the "constitutional" approach to fundamental rights described in this paper. Indeed, Durant, in our view, drives a coach and horses through the law, not so much because of its abstract view of a technical term, but because it will, in effect, allow data controllers to deny data subjects access to their data, and the effective exercise of their rights of correction and erasure, by simply deciding that certain information which they hold is not "personal data" in the sense of the Act. Indeed, they can state that they do not hold any "personal data" on an individual, even though they have information on them on file, which they (the controllers) can readily and easily retrieve by reference to the data subject. We regret the fact that this matter was not referred to

---

278 "*In conformity with the 1981 Convention and the Directive, the purpose of section 7, in entitling an individual to have access to information in the form of his 'personal data' is to enable him to check whether the data controller's processing of it unlawfully infringes his privacy and, if so, to take such steps as the Act provides, for example in sections 10 to 14, to protect it. It is not an automatic key to any information, readily accessible or not, of matters in which he may be named or involved. Nor is to assist him, for example, to obtain discovery of documents that may assist him in litigation or complaints against third parties. As a matter of practicality and given the focus of the Act on ready accessibility of the information - whether from a computerised or comparably sophisticated non-computerised system - it is likely in most cases that only information that names or directly refers to him will qualify. In this respect, **a narrow interpretation of 'personal data' goes hand in hand with a narrow meaning of 'a relevant filing system'**, and for the same reasons (see paragraphs 46-51 below).*" (para. 27 of the judgment, emphasis added). The Court of Appeal then goes on to say, in effect, that even readily available information need not be covered, unless it infringes privacy.

279 Cf. also (again) the comments in the Explanatory Memorandum to the Council of Europe Convention on data protection that the concept of "privacy" as used in that instrument "*is not to be interpreted simply in terms of protection of one's private sphere against intrusive conduct*" but rather "*goes beyond traditional privacy notions*" (paras. 17 and 19).

280 See D. Korff, Data Protection law in the EU, *o.c.* (footnote 1, above), Annex 3, *Comparative Summary*, section 2.1, personal data.

the European Court of Justice for a preliminary ruling and submit that, when in future the Court of Appeal's approach is tested in the European courts (as it undoubtedly will), it will be held to contravene the EC Framework Directive. We will therefore recommend that the Information Commissioner, rather than re-drafting his guidance on the DPA98 to fit in with the Court of Appeal's interpretation, apply the wider, European approach to data protection. Not to do so would fail data subjects, and indeed, in the end, controllers, since the latter are likely to adopt policies now which they will later find to be contrary to European law.

On the remaining issues in Rotaru, the Court, unsurprisingly in view of the earlier case-law mentioned above, held that "*[b]oth the storing of [the information on the applicant] and the use of it, which were coupled with a refusal to allow the applicant an opportunity to refute it, amounted to interference with his right to respect for his private life as guaranteed by Article 8 § 1.*" (para. 46). It also found (with some hesitation) that the storing and use of the information "had a basis in Romanian law" (Law No. 14/1992); and that that law was "foreseeable" since it was published in the Official Gazette (paras. 53 – 54). However, it still had to assess the "quality" of this law, to see if it constituted "law" in the sense in which that word is used in the Convention generally, and Art. 8 in particular:

> "The 'quality' of the legal rules relied on in this case must therefore be scrutinised, with a view, in particular, to ascertaining whether domestic law laid down with sufficient precision the circumstances in which the RIS could store and make use of information relating to the applicant's private life.
>
> The Court notes in this connection that section 8 of Law no. 14/1992 provides that information affecting national security may be gathered, recorded and archived in secret files.
>
> No provision of domestic law, however, lays down any limits on the exercise of those powers. Thus, for instance, the aforesaid Law does not define the kind of information that may be recorded, the categories of people against whom surveillance measures such as gathering and keeping information may be taken, the circumstances in which such measures may be taken or the procedure to be followed. Similarly, the Law does not lay down limits on the age of information held or the length of time for which it may be kept.
>
> Section 45 of the Law empowers the RIS to take over for storage and use the archives that belonged to the former intelligence services operating on Romanian territory and allows inspection of RIS documents with the Director's consent.
>
> The Court notes that this section contains no explicit, detailed provision concerning the persons authorised to consult the files, the nature of the files, the procedure to be followed or the use that may be made of the information thus obtained.
>
> It also notes that although section 2 of the Law empowers the relevant authorities to permit interferences necessary to prevent and counteract threats to national security, the ground allowing such interferences is not laid down with sufficient precision.
>
> The Court must also be satisfied that there exist adequate and effective safeguards against abuse, since a system of secret surveillance designed to protect national security entails the risk of undermining or even destroying democracy on the ground of defending it (see the Klass and Others judgment cited above, pp. 23-24, §§ 49-50).
>
> In order for systems of secret surveillance to be compatible with Article 8 of the Convention, they must contain safeguards established by law which apply to the

> supervision of the relevant services' activities. Supervision procedures must follow the values of a democratic society as faithfully as possible, in particular the rule of law, which is expressly referred to in the Preamble to the Convention. The rule of law implies, *inter alia*, that interference by the executive authorities with an individual's rights should be subject to effective supervision, which should normally be carried out by the judiciary, at least in the last resort, since judicial control affords the best guarantees of independence, impartiality and a proper procedure (see the Klass and Others judgment cited above, pp. 25-26, § 55).
>
> In the instant case the Court notes that the Romanian system for gathering and archiving information does not provide such safeguards, no supervision procedure being provided by Law no. 14/1992, whether while the measure ordered is in force or afterwards.
>
> That being so, the Court considers that domestic law does not indicate with reasonable clarity the scope and manner of exercise of the relevant discretion conferred on the public authorities.
>
> The Court concludes that the holding and use by the RIS of information on the applicant's private life were not 'in accordance with the law', a fact that suffices to constitute a violation of Article 8. Furthermore, in the instant case that fact prevents the Court from reviewing the legitimacy of the aim pursued by the measures ordered and determining whether they were – assuming the aim to have been legitimate – 'necessary in a democratic society'.
>
> There has consequently been a violation of Article 8."
>
> (paras. 56 – 63)

These paragraphs well illustrate the "constitutional" approach to fundamental rights, and data protection. In effect, it provides the Information Commissioner with a "**check-list**" to be followed in assessing the compatibility of (automated or otherwise structured) secret intelligence files (whether held by the secret services or the police) with the fundamental, "constitutional" principles underpinning the Act:

- the Information Commissioner should apply the law (the DPA98) to **all information** in such files directly or indirectly related to identifiable individuals (e.g., not just by name or file number, but also by means of ID numbers, or index numbers, or indeed face-recognition systems). He should emphatically not limit his assessments to information affecting purely private matters, and he should especially not exclude information relating to "activities of a professional or business nature" or to information on political activities or alleged criminal acts, even if of a public nature or carried out in public;

- the Information Commissioner should assess whether there is a **legal basis** for the information-gathering and –retention - but even if that is the case, that is not sufficient: a statute or statutory provision (or exception) authorising the collecting of "information affecting national security" or "relevant to the prevention, investigation or prosecution of criminal offences" is *a necessary, but not a sufficient condition*; rather:

- the Information Commissioner should check whether there exist more **specific legal rules** relating to the **particular kind of processing operation** in question, and if so, whether these rules lay down **appropriate limits** on the statutory powers "such as":

- ✓ a precise description of "the kind of information that may be recorded";

- ✓ a precise description of "the categories of people against whom surveillance measures such as gathering and keeping information may be taken";[281]

- ✓ a precise description of the circumstances in which such measures may be taken;

- ✓ a clearly set out procedure to be followed for the authorisation of such measures;

- ✓ limits on the storing of old information and on the time for which new information can be retained;

- ✓ explicit, detailed provision concerning:

  - ➢ the grounds on which files can be opened;

  - ➢ the procedure to be followed [for opening or accessing the files];

  - ➢ the persons authorised to consult the files;

  - ➢ the nature of the files;

  - ➢ the use that may be made of the information in the files;

  NB: Such rules can be set out in subsidiary rules or regulations - but in order to qualify as "law" in Convention terms, they must be **published**.

- Next, the Information Commissioner should check whether there are "safeguards established by law" which ensure "**appropriate [and effective] supervision** of the relevant services' activities". This supervision should "normally" be carried out by the judiciary (if it is not, there should be particularly strong alternative supervisory mechanisms, such as close Parliamentary scrutiny: cf. the Klass- and Kopp-judgments referred to in the Rotaru-judgment).

It may again be noted that the latter, procedural (supervision) requirement is seen as part of the test of whether the legal rule in question has the appropriate quality. But the existence of such procedures is of course also essential in the assessment of compliance with Art. 13 ECHR (the right to an effective remedy before a national authority).

---

[281] Note that the Court here clearly regards the gathering and keeping of information for intelligence files as, as such, "surveillance measures". This is not qualified by reference to the means used: "surveillance" is not limited to secret, technical means; it can also be kept on individuals by collecting information openly, or from public sources, e.g. from lists signed by people opposing the War In Iraq, or newspaper cuttings, or open photograhy or videoing of demonstrations.

It may suffice to note the general points made in this respect by the Court, again with reference to earlier case-law. First of all, the Court confirmed that a remedy should be available to anyone with an "arguable claim" of a violation of a Convention right: there is no need to show that an actual violation has occurred. In the case at hand, it was clear that there was, at least, such an "arguable" case, and the applicant was therefore entitled to an effective domestic remedy within the meaning of Article 13 of the Convention (paras. 67 – 68).

As to the nature of the "authority" responsible for providing the remedy in cases of secret intelligence data, the Court said that:

> "The 'authority' referred to in Article 13 may not necessarily in all instances be a judicial authority in the strict sense. Nevertheless, the powers and procedural guarantees an authority possesses are relevant in determining whether the remedy before it is effective (see the Klass and Others judgment cited above, p. 30, § 67). Furthermore, where secret surveillance is concerned, objective supervisory machinery may be sufficient as long as the measures remain secret. It is only once the measures have been divulged that legal remedies must become available to the individual (ibid., p. 31, §§ 70-71)."
>
> (para. 69)

In the case of the applicant, the information had been disclosed, but:

> "... neither the provisions relied on by the respondent Government nor any other provisions of that Law make it possible to challenge the holding, by agents of the State, of information on a person's private life or the truth of such information. The supervisory machinery established by sections 15 and 16 relate only to the disclosure of information about the identity of some of the *Securitate*'s collaborators and agents.
>
> The Court has not been informed of any other provision of Romanian law that makes it possible to challenge the holding, by the intelligence services, of information on the applicant's private life or to refute the truth of such information.
>
> The Court consequently concludes that the applicant has been the victim of a violation of Article 13."
>
> (paras. 71 – 73)

This merely confirms that approach of the Court with regard to the procedural aspect of Art. 8, noted above, according to which there can be alternative, internal, non-judicial mechanisms to supervise the collecting, retention and internal use of intelligence data - but that (1) it is important that such mechanisms, in spite of not being open and judicial, should nevertheless be independent and effective; and (2) that if and when previously secret intelligence data are disclosed, the data subject should have access to a judicial remedy.

Finally, it may be noted that the applicant had sought damages through the civil courts, but that the courts had not granted such relief, even though that clearly had jurisdiction. The Court (again, not surprisingly) found that this violated Mr. Rotaru's right to a fair trial (paras. 74 – 79). It awarded 50,000 French Francs in damages, plus costs (paras. 84 – 88).

2.2.6 Case-law of the European Court of Justice

The EC Framework Directive on data protection (Directive 95/46/EC) had to be implemented by the Member States by October 1998. In fact, many of the Member States took considerably longer to do so. Apart from infringement procedures brought by the European Commission against a number of States for non-implementation,[282] there have therefore, to date, only been a few cases before the European Court of Justice (ECJ) relating to the substance (and scope) of the Directive. These cases are, however, of particular interest; they confirm the "constitutional" approach to data protection we discerned in the case-law of the European Court of Human Rights.

Before discussing these, and without going into detail, it may be reiterated, first of all, that the substantive requirements of the European Convention on Human Rights constitute "general principles of Community law", of overriding, constitutional importance within the legal order of the Community (and indeed the Union). This was first expressly stated (as far as EC law was concerned) in the second Nold-case (Case 4/73 [1974], ECR 491) and has since been confirmed explicitly in the Treaty on European Union (see Art. 6 TEU, formerly Art. F.2). As already noted, this is further emphasised by the adoption of the Charter (which builds on the ECHR) and will be yet further confirmed (for the whole Union) if the proposed Constitution is adopted as proposed.[283]

Secondly, the European Court of Justice has expressly held that:

> "where national legislation falls within the field of application of Community law the Court, in a reference for a preliminary ruling, must give the national court all the guidance as to interpretation necessary to enable it to assess the compatibility of that legislation with the fundamental rights - as laid down in particular in the [European Convention on Human Rights] - whose observance the Court ensures." [284]

In other words, because the substantive provisions of the ECHR are an integral part of EC- and EU-law, the ECJ feels competent - indeed, obliged - to apply, and where necessary explain the application and interpretation of, the Human Rights Convention in relevant cases.

Thirdly, certain provisions of Community law may be "directly applicable" - which means that they can be invoked directly in the domestic courts, even in the absence of national legislation implementing those provisions (or if individuals feel that the national legislation purporting to implement those provisions in fact fails to do so, or to do so fully). With regard to data protection, the question therefore arises whether the general principles and criteria, and/or certain specific provisions, of the EC Framework Directive on data protection enjoy this status.

Two cases relating to the EC Framework Directive on data protection are of particular interest in these regards. They both concern "preliminary rulings" on questions of law. This means that the Court's rulings are intended to guide the national courts on how to apply the relevant principles; the Court thus, in several respects, stresses that the specific application of those

---

282 Cf. the Court's judgment of 4 October 2001 in case C-450/00 against Luxembourg.

283 For references to these constitutional documents, see footnotes 7 and 22, above. For further detail on the development of human rights in the EC and the EU, see D Korff, *Human rights in the European Union*, Cambridge\Bilbao, June 1994.

284 Note (Judgment of 29 May 1997 in the Kremzow Case, Case C-229/95, para. 15).

principles to the particular facts of individual cases is left to the national courts, taking into account the rulings of the Court. Similarly, the Information Commissioner should follow the approach indicated by the ECJ: He is left with a margin of appreciation on how to exercise his powers, as long as he does so in accordance with the approach and principles indicated.

The first case to be noted is the case of Österreichischer Rundfunk v. Austria.[285] It concerned the obligation of public bodies subject to control by the *Rechnungshof* (the Austrian Court of Audit) to communicate to the latter details of the salaries and pensions exceeding a certain level paid by them to their employees and pensioners together with the names of the recipients, for the purpose of drawing up an annual report to be transmitted to the *Nationalrat*, the *Bundesrat* and the *Landtage* (the lower and upper chambers of the Federal Parliament and the provincial assemblies) and made available to the general public.[286] *Österreichischer Rundfunk* (ÖRF, Austrian Radio), which is one such body, and several other bodies, refused to disclose this information to the *Rechnungshof* (other than in anonymised form), because if felt that to do otherwise would infringe the right to private life of the employees in question, contrary to Art. 8 ECHR and to the EC Framework Directive. Several employees of ÖRF also sought injunctions against the disclosure of their data, on the same grounds.[287] Both the Constitutional Court and the Supreme Court referred the matter to the ECJ, which joined the cases.

In its preliminary ruling the Court notes first of all, clearly and simply:

> "... that the data at issue in the main proceedings, which relate both to the monies paid by certain bodies and the recipients, constitute personal data within the meaning of Article 2(a) of Directive 95/46, being information relating to an identified or identifiable natural person."

and that:

> "Their recording and use by the body concerned, and their transmission to the Rechnungshof and inclusion by the latter in a report intended to be communicated to various political institutions and widely diffused, constitute processing of personal data within the meaning of Article 2(b) of the directive."
>
> (para. 64)

Neither here nor in the passage quoted below does the Court in any way qualify the concept of "personal data": it clearly regards *any* information relating to an identified or identifiable natural person as such (in contrast, again, to the UK Court of Appeal's ruling in Durant). If anything, as shown below, the ECJ, like the European Court of Human Rights, stresses the need to give the term a *wide* meaning.

---

285 Joined Cases C-465/00 (Rechnungshof v. ÖRF *et al.*), C-138/01 and C-139/01 (respectively, Christa Neukomm and Lauermann v. ÖRF) (references for preliminary rulings from the Austrian *Verfassungsgerichtshof* and *Oberster Gerichtshof* respectively), Opinion of Advocate-General Tizzano of 14 November 2002; Judgment of 20 May 2003.

286 The obligation was imposed by the Bundesverfassungsgesetz über die Begrenzung von Bezügen öffentlicher Funktionäre (Federal constitutional law on the limitation of salaries of public officials, BGBl. I 1997/64, as amended) or BezBegrBVG for short.

287 The case also hinged (as a further preliminary matter) on whether the obligation of publicity created a barrier to the movement of workers, contrary to Article 39 ECT. While this is of course a crucial issue in terms of Community law, it does not affect the broader issues addressed in this paper. This issue will therefore not be discussed here, other than to note that the Court held that "the applicability of Directive 95/46 cannot depend on whether the specific situations at issue in the main proceedings have a sufficient link with the exercise of the fundamental freedoms guaranteed by the Treaty, in particular, in those cases, the freedom of movement of workers." (para. 43; see also paras. 44 – 47).

The Court then goes on to analyse the case at hand in accordance with the typical, standard "constitutional" approach first adopted by the European Court of Human Rights, described under the previous heading. In order to show the clear acceptance, by the ECJ, of this "Strasbourg approach" in relation to human rights-related cases under Community law, it is useful to quote the analysis of the ECJ in this respect in full:

> "65. Under Directive 95/46, subject to the exceptions permitted under Article 13, all processing of personal data must comply, first, with the principles relating to data quality set out in Article 6 of the directive and, second, with one of the criteria for making data processing legitimate listed in Article 7.
>
> 66. More specifically, the data must be collected for specified, explicit and legitimate purposes (Article 6(1)(b) of Directive 95/46) and must be adequate, relevant and not excessive in relation to those purposes (Article 6(1)(c)). In addition, under Article 7(c) and (e) of the directive respectively, the processing of personal data is permissible only if it is necessary for compliance with a legal obligation to which the controller is subject or is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller ... to whom the data are disclosed.
>
> 67. However, under Article 13(e) and (f) of the directive, the Member States may derogate *inter alia* from Article 6(1) where this is necessary to safeguard respectively an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters or a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in particular cases including that referred to in subparagraph (e).
>
> 68. It should also be noted that the provisions of Directive 95/46, in so far as they govern the processing of personal data liable to infringe fundamental freedoms, in particular the right to privacy, must necessarily be interpreted in the light of fundamental rights, which, according to settled case-law, form an integral part of the general principles of law whose observance the Court ensures (see, *inter alia*, Case C-274/99 P *Connolly* v *Commission* [2001] ECR I-1611, paragraph 37).
>
> 69. Those principles have been expressly restated in Article 6(2) EU, which states that [t]he Union shall respect fundamental rights, as guaranteed by the [Convention] and as they result from the constitutional traditions common to the Member States, as general principles of Community law.
>
> 70. Directive 95/46 itself, while having as its principal aim to ensure the free movement of personal data, provides in Article 1(1) that Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data. Several recitals in its preamble, in particular recitals 10 and 11, also express that requirement.
>
> 71. In this respect, it is to be noted that Article 8 of the Convention, while stating in paragraph 1 the principle that the public authorities must not interfere with the right to respect for private life, accepts in paragraph 2 that such an interference is possible where it is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.
>
> 72. So, for the purpose of applying Directive 95/46, in particular Articles 6(1)(c), 7(c) and (e) and 13, it must be ascertained, first, whether legislation such as that at issue in the

main proceedings provides for an interference with private life, and if so, whether that interference is justified from the point of view of Article 8 of the Convention.

Existence of an interference with private life

73. First of all, the collection of data by name relating to an individual's professional income, with a view to communicating it to third parties, falls within the scope of Article 8 of the Convention. **The European Court of Human Rights has held in this respect that the expression private life must not be interpreted restrictively and that there is no reason of principle to justify excluding activities of a professional ... nature from the notion of private life** (see, *inter alia*, *Amann v. Switzerland* [GC], no. 27798/95, § 65, ECHR 2000-II and *Rotaru v. Romania* [GC], no. 28341/95, § 43, ECHR 2000-V).

74. It necessarily follows that, while the mere recording by an employer of data by name relating to the remuneration paid to his employees cannot as such constitute an interference with private life, the communication of that data to third parties, in the present case a public authority, infringes the right of the persons concerned to respect for private life, whatever the subsequent use of the information thus communicated, and constitutes an interference within the meaning of Article 8 of the Convention.

75. To establish the existence of such an interference, it does not matter whether the information communicated is of a sensitive character or whether the persons concerned have been inconvenienced in any way (see, to that effect, *Amann v. Switzerland*, § 70). It suffices to find that data relating to the remuneration received by an employee or pensioner have been communicated by the employer to a third party.

Justification of the interference

76. An interference such as that mentioned in paragraph 74 above violates Article 8 of the Convention unless it is in accordance with the law, pursues one or more of the legitimate aims specified in Article 8(2), and is necessary in a democratic society for achieving that aim or aims.

77. It is common ground that the interference at issue in the main proceedings is in accordance with Paragraph 8 of the BezBegrBVG. However, the question arises whether that paragraph is formulated with sufficient precision to enable the citizen to adjust his conduct accordingly, and so complies with the requirement of foreseeability laid down in the case-law of the European Court of Human Rights (see, *inter alia*, *Rekvényi v. Hungary* [GC], no. 25390/94, § 34, ECHR 1999-III).

78. In this respect, Paragraph 8(3) of the BezBegrBVG states that the report drawn up by the Rechnungshof is to include all persons whose total yearly salaries and pensions from bodies ... exceed the amount stated in subparagraph 1, without expressly requiring the names of the persons concerned to be disclosed in relation to the income they receive. According to the orders for reference, it is legal commentators who, on the basis of the *travaux préparatoires*, interpret the constitutional law in that way.

79. It is for the national courts to ascertain whether the interpretation to the effect that Paragraph 8(3) of the BezBegrBVG requires disclosure of the names of the persons concerned in relation to the income received complies with the requirement of foreseeability referred to in paragraph 77 above.

80. However, that question need not arise until it has been determined whether such an interpretation of the national provision at issue is consistent with Article 8 of the Convention, as regards its required proportionality to the aims pursued. That question will be examined below.

81. It appears from the order for reference in Case C-465/00 that the objective of Paragraph 8 of the BezBegrBVG is to exert pressure on the public bodies concerned to keep salaries within reasonable limits. **The Austrian Government observes, more generally, that the interference provided for by that provision is intended to guarantee the thrifty and appropriate use of public funds by the administration. Such an objective constitutes a legitimate aim within the meaning both of Article 8(2) of the Convention, which mentions the economic well-being of the country, and Article 6(1)(b) of Directive 95/46, which refers to specified, explicit and legitimate purposes.**

82. It must next be ascertained whether the interference in question is necessary in a democratic society to achieve the legitimate aim pursued.

83. According to the European Court of Human Rights, the adjective necessary in Article 8(2) of the Convention implies that a pressing social need is involved and that the measure employed is proportionate to the legitimate aim pursued (see, *inter alia*, the Gillow v. the United Kingdom judgment of 24 November 1986, Series A no. 109, § 55). The national authorities also enjoy a margin of appreciation, the scope of which will depend not only on the nature of the legitimate aim pursued but also on the particular nature of the interference involved (see the Leander v. Sweden judgment of 26 March 1987, Series A no. 116, § 59).

84. The interest of the Republic of Austria in ensuring the best use of public funds, and in particular keeping salaries within reasonable limits, must be balanced against the seriousness of the interference with the right of the persons concerned to respect for their private life.

85. On the one hand, in order to monitor the proper use of public funds, the Rechnungshof and the various parliamentary bodies undoubtedly need to know the amount of expenditure on human resources in the various public bodies. In addition, in a democratic society, taxpayers and public opinion generally have the right to be kept informed of the use of public revenues, in particular as regards expenditure on staff. Such information, put together in the Report, may make a contribution to the public debate on a question of general interest, and thus serves the public interest.

86. The question nevertheless arises whether stating the names of the persons concerned in relation to the income received is proportionate to the legitimate aim pursued and whether the reasons relied on before the Court to justify such disclosure appear relevant and sufficient.

87. It is plain that, according to the interpretation adopted by the national courts, Paragraph 8 of the BezBegrBVG requires disclosure of the names of the persons concerned, in relation to income above a certain level, with respect not only to persons filling posts remunerated by salaries on a published scale, but to all persons remunerated by bodies subject to control by the Rechnungshof. Moreover, such information is not only communicated to the Rechnungshof and via the latter to the various parliamentary bodies, but is also made widely available to the public.

88. It is for the national courts to ascertain whether such publicity is both necessary and proportionate to the aim of keeping salaries within reasonable limits, and in particular to

examine whether such an objective could not have been attained equally effectively by transmitting the information as to names to the monitoring bodies alone. Similarly, the question arises whether it would not have been sufficient to inform the general public only of the remuneration and other financial benefits to which persons employed by the public bodies concerned have a contractual or statutory right, but not of the sums which each of them actually received during the year in question, which may depend to a varying extent on their personal and family situation.

89. With respect, on the other hand, to the seriousness of the interference with the right of the persons concerned to respect for their private life, it is not impossible that they may suffer harm as a result of the negative effects of the publicity attached to their income from employment, in particular on their prospects of being given employment by other undertakings, whether in Austria or elsewhere, which are not subject to control by the Rechnungshof.

90. It must be concluded that the interference resulting from the application of national legislation such as that at issue in the main proceedings may be justified under Article 8(2) of the Convention only in so far as the wide disclosure not merely of the amounts of the annual income above a certain threshold of persons employed by the bodies subject to control by the Rechnungshof but also of the names of the recipients of that income is both necessary for and appropriate to the aim of keeping salaries within reasonable limits, that being a matter for the national courts to examine.

Consequences with respect to the provisions of Directive 95/46

91. If the national courts conclude that the national legislation at issue is incompatible with Article 8 of the Convention, that legislation is also incapable of satisfying the requirement of proportionality in Articles 6(1)(c) and 7(c) or (e) of Directive 95/46. Nor could it be covered by any of the exceptions referred to in Article 13 of that directive, which likewise requires compliance with the requirement of proportionality with respect to the public interest objective being pursued. In any event, that provision cannot be interpreted as conferring legitimacy on an interference with the right to respect for private life contrary to Article 8 of the Convention.

92. If, on the other hand, the national courts were to consider that Paragraph 8 of the BezBegrBVG is both necessary for and appropriate to the public interest objective being pursued, they would then, as appears from paragraphs 77 to 79 above, still have to ascertain whether, by not expressly providing for disclosure of the names of the persons concerned in relation to the income received, Paragraph 8 of the BezBegrBVG complies with the requirement of foreseeability.

93. Finally, it should be noted, in the light of the above considerations, that the national court must also interpret any provision of national law, as far as possible, in the light of the wording and the purpose of the applicable directive, in order to achieve the result pursued by the latter and thereby comply with the third paragraph of Article 249 EC (see Case C-106/89 *Marleasing* [1990] ECR I-4135, paragraph 8).

94. In the light of all the above considerations, the answer to the first question must be that Articles 6(1)(c) and 7(c) and (e) of Directive 95/46 do not preclude national legislation such as that at issue in the main proceedings, provided that it is shown that the wide disclosure not merely of the amounts of the annual income above a certain threshold of persons employed by the bodies subject to control by the Rechnungshof but also of the names of the recipients of that income is necessary for and appropriate to the objective of

> proper management of public funds pursued by the legislature, that being for the national courts to ascertain."
>
> (Judgment, paras. 65 – 94, emphasis added)

It should be noted that the Court not only follows the "Strasbourg approach" in a general sense, by applying the various tests adduced by the European Court of Human Rights, in basically the same order,[288] but in fact **identifies** the tests to be applied under Community law with the ones applied under the Human Rights Convention: as is made clear in para. 91 of the judgment, quoted above, legislation which violates Art. 8 ECHR also, *ipso facto* violates the basic data protection principles and –criteria set out in the Framework Directive; and States cannot rely on the exception clause in the Framework Directive (Art. 13) to depart from the basic data protection principles and criteria in ways that would not conform to the second paragraph of Art. 8 of the Human Rights Convention.[289]

The national authorities are allowed to form their own judgment on specific matters before them - provided this is done in the way indicated. Indeed, the observations of the Court in respect of the matters to be taken into account under the Austrian law on the disclosure of income data (paras. 88 – 89 above) clearly suggests that if less intrusive means can be found to achieve the aim of public thrift, those less-intrusive means must be chosen: otherwise, the Austrian courts would have to strike out the statutory requirements in question.

We will see below that the ECJ has confirmed these matters in the second case to be considered. First, however, we must note that the importance of EC law in this respect is further enhanced by the fact that the Luxembourg Court has ruled, in the ÖRF-case, that the basic data protection principles and -criteria set out in the Framework Directive are **directly applicable** and may therefore be invoked by individuals in the domestic courts (including of course the courts in the UK):

> **The second question**
>
> 95. By their second question, the national courts ask whether the provisions of Directive 95/46 which preclude national legislation such as that at issue in the main proceedings are directly applicable, in that they may be relied on by individuals before the national courts to oust the application of that legislation.
>
> 96. The defendants in the main proceedings in Case C-465/00 and the Netherlands Government consider that Articles 6(1) and 7 of Directive 95/46 fulfil the criteria stated in the Court's case-law for having such direct effect. They are sufficiently precise and unconditional for the bodies required to disclose the data relating to the income of the persons concerned to be able to rely on them to prevent application of the national provisions contrary to those provisions.
>
> 97. The Austrian Government submits, on the other hand, that the relevant provisions of Directive 95/46 are not directly applicable. In particular, Articles 6(1) and 7 are not unconditional, since their implementation requires the

---

[288] The ECJ slightly departs from the "Strasbourg" sequence, in that it defers, in thia case, the question of whether the legal rules in question were sufficiently "foreseeable" - and thus, whether the interference was "in accordance with law" in the Convention sense - until after its examination of the "necessity" and "proportionality" of the interference.

[289] We will discuss below, under the next heading, the exclusion of certain so-called "Third Pillar" matters (such as processing relating to national security or police activities) from the Framework Directive, and argue that that exclusion is not important to the Information Commissioner in his work.

> Member States, which have a wide discretion, to adopt special measures to that effect.
>
> 98. On this point, it should be noted that wherever the provisions of a directive appear, so far as their subject-matter is concerned, to be unconditional and sufficiently precise, they may, in the absence of implementing measures adopted within the prescribed period, be relied on against any national provision which is incompatible with the directive or in so far as they define rights which individuals are able to assert against the State (see, *inter alia*, Case 8/81 *Becker* [1982] ECR 53, paragraph 25, and Case C-141/00 *Bugler* [2002] ECR I-6833, paragraph 51).
>
> **99. In the light of the answer to the first question, the second question seeks to know whether such a character may be attributed to Article 6(1)(c) of Directive 95/46, under which personal data must be ... adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed, and to Article 7(c) or (e), under which personal data may be processed only if *inter alia* processing is necessary for compliance with a legal obligation to which the controller is subject or is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller ... to whom the data are disclosed.**
>
> **100. Those provisions are sufficiently precise to be relied on by individuals and applied by the national courts. Moreover, while Directive 95/46 undoubtedly confers on the Member States a greater or lesser discretion in the implementation of some of its provisions, Articles 6(1)(c) and 7(c) or (e) for their part state unconditional obligations.**
>
> **101. The answer to the second question must therefore be that Articles 6(1)(c) and 7(c) and (e) of Directive 95/46 are directly applicable, in that they may be relied on by an individual before the national courts to oust the application of rules of national law which are contrary to those provisions."**
>
> (Judgment, paras. 95 – 101, emphasis added)

This means that individuals in the UK may directly rely on Arts. 6 and 7 of the Framework Directive in any claims they may wish to make about the processing of their personal data. The courts - and thus, of course, also the Information Commissioner - are obliged to apply these provisions, and if needs be set aside even formal statutory provisions (as well of course as any lower rules or regulations) which fail to conform to those principles. Indeed, we submit that the UK courts are also obliged to apply the term "personal data", already, in the wider sense in which that term is used in the EC Directive - and that Durant therefore also contravenes European Community law. The Information Commissioner is thus, in our view, obliged to disregard the Court of Appeal's narrow ruling and instead give broad and strong protection to individuals on the basis of the broad data protection principles and –criteria set out in the Directive. Also and in particular in relation to the processing of personal data for law enforcement purposes, the Commissioner should not defer to national provisions overriding basic rules in the DPA98 and/or the Framework Directive, but rather, should only apply those provisions to the extent that they are compatible with the Directive and the ECHR. In this, he may (and should) of course take account of the exceptions clauses in these instruments - but these too should be applied in accordance with the general approach and

specific tests adduced by the European courts. That is the implication of the UK rules being so deeply embedded in the European ones.

The second case to be mentioned is the case of Linqvist v Sweden.[290] The facts in the case are straight-forward; they are set out by the Advocate-General in his Opinion on the case as follows:

> "In autumn 1998, in addition to her normal job, Mrs Bodil Lindqvist was carrying out voluntary work as a catechist in the parish of Alseda in Sweden. In the course of her work, to enable the parishioners to obtain easily the information they needed, Mrs Lindqvist set up a home page on the Internet with information about herself, her husband and 16 colleagues in the parish, giving only their first name in some cases and their full name in others. In addition, the home page described, in a mildly humorous manner, her colleagues' jobs and hobbies; and in some cases their family circumstances were outlined, and telephone numbers and other personal information given. One of the various items of interest for present purposes was a report that a colleague was on half-time on medical grounds because she had injured her foot. The home page was also accessible through the Swedish Church's home page, with which a link had been set up at Mrs Lindqvist's request.
>
> Mrs Lindqvist had not told her colleagues about the home page or sought their consent to process their data. The *Datainspektionen* [the Swedish data protection authority] had not been informed that the home page was being set up, nor had it been notified of any processing of personal data. The home page was short-lived, however, as Mrs Lindqvist quickly took steps to remove it as soon as she became aware that some of her colleagues were unhappy about it.
>
> Although the home page was removed promptly, Mrs Lindqvist was prosecuted in Sweden under Paragraph 49(1)(b) to (d) of the *Personuppgiftslagen* [the Swedish Data Protection Law] for setting it up. It was claimed in particular that she had processed data by automatic means without giving prior written notification to the *Datainspektionen*; that she had processed sensitive data, such as the data relating to her colleague's injury and subsequent half-time employment on medical grounds; and that she had transferred processed personal data to a third country without authorisation."
>
> (A-G Opinion, paras. 17 – 19; cf. Judgment, paras. 12 – 15)[291]

On the question of whether Mrs. Lindqvist's activities fell within the ambit of the Framework Directive, the Court (in line with its broad interpretations of the relevant terms in the ÖRF-case), first of all reiterated that

> "The term personal data used in Article 3(1) of Directive 95/46 covers, according to the definition in Article 2(a) thereof, any information relating to an identified or identifiable natural person. The term undoubtedly covers the name of a person in conjunction with his telephone coordinates or information about his working conditions or hobbies.
>
> According to the definition in Article 2(b) of Directive 95/46, the term processing of such data used in Article 3(1) covers any operation or set of operations which is performed

---

290 Case C-101/01 Bodil Lindqvist v Åklagarkammaren i Jönköping (Reference for a preliminary ruling from the Göta Hovrätt), Opinion of Advocate-General Tizzano of 19 September 2002; Judgment of 6 November 2003.

291 According to the judgment, the home page contained information relating to Mrs. Lindqvist and 18 colleagues (para. 13).

> upon personal data, whether or not by automatic means. That provision gives several examples of such operations, including disclosure by transmission, dissemination or otherwise making data available. It follows that the operation of loading personal data on an internet page must be considered to be such processing.
>
> It remains to be determined whether such processing is wholly or partly by automatic means. In that connection, placing information on an internet page entails, under current technical and computer procedures, the operation of loading that page onto a server and the operations necessary to make that page accessible to people who are connected to the internet. Such operations are performed, at least in part, automatically.
>
> The answer to the first question must therefore be that the act of referring, on an internet page, to various persons and identifying them by name or by other means, for instance by giving their telephone number or information regarding their working conditions and hobbies, constitutes the processing of personal data wholly or partly by automatic means within the meaning of Article 3(1) of Directive 95/46."
>
> (Judgment, paras. 24 – 27)

The Court next held that Mrs Linqvist activities did not fall either within the exception contained in Art. 3(2), first indent, of the Directive, relating to state security, defence, police matters etc. (para. 43 – 45, further discussed under the next heading), or within the other exception in that article, concerning processing of personal data for "purely personal or household" activities:

> "As regards the exception provided for in the second indent of Article 3(2) of Directive 95/46, the 12th recital in the preamble to that directive, which concerns that exception, cites, as examples of the processing of data carried out by a natural person in the exercise of activities which are exclusively personal or domestic, correspondence and the holding of records of addresses.
>
> That exception must therefore be interpreted as relating only to activities which are carried out in the course of private or family life of individuals, which is clearly not the case with the processing of personal data consisting in publication on the internet so that those data are made accessible to an indefinite number of people.
>
> The answer to the third question must therefore be that processing of personal data such as that described in the reply to the first question is not covered by any of the exceptions in Article 3(2) of Directive 95/46."
>
> (paras. 46 – 48)

There was also no doubt that the information about the injury to a named person's foot constituted medical, and thus "sensitive", data (paras. 49 – 51).

In reply to the argument of Mrs. Linqvist that she has been unduly restricted in her right to disseminate information, the Court stressed that data protection and the freedom to disseminate information had to be balanced against each other, and that it was primarily a matter for the domestic authorities to strike this balance. The provisions of the Framework Directive were sufficiently flexible to allow for this:

> "the provisions of Directive 95/46 do not, in themselves, bring about a restriction which conflicts with the general principles of freedom of expression or other freedoms and rights, which are applicable within the European Union and are enshrined inter alia in Article 10 of the ECHR. It is for the national authorities and courts responsible for applying the national legislation implementing Directive 95/46 to ensure a fair balance between the rights and interests in question, including the fundamental rights protected by the Community legal order."
>
> (para. 90)

Finally,[292] the Court examined the question of whether Member States could offer more extensive protection than envisaged by the Framework Directive. In this regard, the Court observed that, within its area of applicability (i.e. within the scope of Community law, subject to the exceptions in Art. 3(2) discussed above), the Member States have only a very limited margin to go beyond what is stipulated in the Directive:

> "Directive 95/46 is intended, as appears from the eighth recital in the preamble thereto, to ensure that the level of protection of the rights and freedoms of individuals with regard to the processing of personal data is equivalent in all Member States. The tenth recital adds that the approximation of the national laws applicable in this area must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the Community.
>
> The harmonisation of those national laws is therefore not limited to minimal harmonisation but amounts to harmonisation which is generally complete. It is upon that view that Directive 95/46 is intended to ensure free movement of personal data while guaranteeing a high level of protection for the rights and interests of the individuals to whom such data relate.
>
> It is true that Directive 95/46 allows the Member States a margin for manoeuvre in certain areas and authorises them to maintain or introduce particular rules for specific situations as a large number of its provisions demonstrate. However, such possibilities must be made use of in the manner provided for by Directive 95/46 and in accordance with its objective of maintaining a balance between the free movement of personal data and the protection of private life."
>
> (paras. 95 – 97)

However, they have more freedom as concerns matters outside the scope of the Directive:

> "On the other hand, nothing prevents a Member State from extending the scope of the national legislation implementing the provisions of Directive 95/46 to areas not included

---

[292] We are not discussing here the penultimate question addressed by the Court: "*whether loading personal data onto an internet page constitutes a transfer of those data to a third country within the meaning of Article 25 of Directive 95/46 merely because it makes them accessible to people in a third country?*" The reply of the Court, to the effect that there is no such transfer if "*an individual in a Member State loads personal data onto an internet page which is stored with his hosting provider which is established in that State or in another Member State*" (para. 71) is, in the light of current technology, perhaps surprising, but it does not affect the issues addressed in this study.

> within the scope thereof, provided that no other provision of Community law precludes it."
>
> (para. 98)

The above makes clear that, in the view of the European Court of Justice, data protection is a fundamental, constitutional issue: the principles of the Framework Directive must be construed as fundamental, constitutional human rights principles, and applied in accordance with the case-law of the European Court of Human Rights. More specifically, the ECJ has clearly endorsed, and adopted for itself, the typical, "standard" approach to human rights developed by the Strasbourg Court - and follows this approach also and in particular in its assessment of cases relating to the Framework Directive.

However, as already noted, the Framework Directive is itself limited in scope. Before turning to the way in which data protection has been applied by the Working Party and the national data protection authorities (below, at 3), we must therefore first discuss the implications - or rather, as we shall show, the irrelevance - of this limitation on the scope of the Framework Directive for the matters discussed in this study.

2.2.7 The irrelevance, for the UK Information Commissioner, of the distinction between activities relating to the different "pillars" of the EU

The ÖRF-case, discussed above, concerned exceptions to the "purpose-limitation principle" and processing on the basis of a legal duty rather than with the consent of the data subjects (indeed even against their express wishes). As noted, the Court therefore examined the applicability of the exception clause in the Framework Directive, Art. 13, and held that the processing in question was aimed at protecting the economic well-being of the country, before then applying the various "Strasbourg" tests to such exceptions.

In principle, the Court's reasoning in this respect equally applies to the other purposes for which, under Art. 13, exceptions may be imposed on the basic provisions of the Directive (or rather, of the national laws implementing the Directive, including the UK DPA98), such as **national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences**.

Against this could be said that these matters fall outside the scope of the Framework Directive, which expressly does not apply to the processing of personal data:

> "in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law" (Art. 3(2), first indent)[293]

However, two matters should be noted. First of all, this limitation of the scope of the Directive must (because it limits human rights protection) be strictly interpreted. It does not generally cover processing operations by private-sector controllers, even though these may relate to the matters listed. As the Court put it in the Linqvist case, discussed above:

---

[293] The second main exception set out in Art. 3(2) of the Framework Directive concerns processing for "purely personal or household" activities, as discussed with regard to the Linqvist case, above.

> "The activities mentioned by way of example in the first indent of Article 3(2) of Directive 95/46 (in other words, the activities provided for by Titles V and VI of the Treaty on European Union and processing operations concerning public security, defence, State security and activities in areas of criminal law) are, in any event, activities of the State or of State authorities and unrelated to the fields of activity of individuals."
>
> (Lindqvist-judgment, para. 43)

The non-applicability of the first indent of Art. 3(2) to private actors has also been made clear as concerns the proposal that communication service providers and ISPs be compelled to retain communication data which no longer serve their initial purposes, for the benefit of law enforcement and anti-terrorist operations. It is manifest from the detailed opinions of the Working Party and of national data protection authorities that such data retention *is* subject to the provisions of the Framework Directive. In particular, the need for such duties is examined by them in the light of Art. 13: if the matter fell outside the scope of the Directive, it couldn't be subject to that assessment.

Secondly, and more fundamentally, the above-mentioned restriction on the scope of the Directive is merely a consequence of the fact that it is an *EC* Directive: the matters indicated in Art. 3(2) are outside the scope of European Community law and cannot therefore be regulated in a legal instrument adopted with a view to facilitating the operation of the internal market. Article 3(2) should not be seen as an indication that the matters listed need not be subject to strict data protection rules. On the contrary, as the Charter and (in the near future) the Constitution make clear, data protection should apply "seamlessly", to all areas of EU law.

This is explicitly also the view of the European Parliament, as set out in its very recent (February 2004) report on the implementation of the Directive.[294] Parliament stresses that "*the right to privacy is a fundamental human right, as set out in all the main legal instruments that guarantee citizens' freedoms and rights at international, European and national level*" and notes that "*the EU has developed a legal regime aimed at guaranteeing citizens' privacy through a high standard of data protection in areas covered by the first pillar.*"[295] However:

> "due to the current pillar structure of the EU, activities that fall within the remit of the second and third pillars are excluded from this legal regime and are partially subject to fragmented specific provisions; ... the European Parliament is only partially consulted and informed and ... the Court of Justice has limited powers in this area."[296]

Parliament therefore stressed:

> "**the need for a comprehensive and trans-pillar European privacy and data protection regime**
>
> [Parliament]

---

294 Report on the First Report on the implementation of the Data Protection Directive (95/46/EC) (COM(2003) 265 – C5-0375/2003 – 2003/2153(INI)), Document A5-0104/2004 (Final), Committee on Citizens' Freedoms and Rights, Justice and Home Affairs, 24 February 2004.

295 *Idem*, p.6, at A. and B.

296 *Idem*, p. 6, at C.

> 1. Deplores the extremely serious delays that have occurred within the Commission in this matter and urges it to propose within the first half of 2004, as announced, a 'legal instrument' on the protection of privacy in the third pillar; this instrument should be binding in nature and aimed at guaranteeing in the third pillar the same level of data protection and privacy rights as in the first pillar; it should harmonise, according to these high standards, the current rules on privacy and data protection concerning Europol, Eurojust and all other third-pillar organs and actions, as well as any exchange of data between them and with third countries and organisations;
>
> 2. Considers that, in the long term, Directive 95/46/EC should be applied, following the appropriate modifications, to cover all areas of EU activity, so as to guarantee a high standard of harmonised and common rules for privacy and data protection;
>
> 3. Believes that respect for privacy and data protection rules should be guaranteed by national supervisory authorities, a common EU authority, to which citizens will have the right to appeal, and the Court of Justice ..."[297]

It may also be noted that a study for the European Commission concluded that:

> "... 'seamless' implementation of the Directive, to matters both within and without the scope of Community law, is eminently 'feasible'. It would underline rather than undermine crucial constitutional requirements in many Member States. It would avoid the serious legal and practical problems which the 'seams' resulting from partial implementation would create. It would avoid possible conflicts between national constitutional and European legal requirements; and it would facilitate rather than hamper data exchanges relating to European matters outside of Community law such as, in particular, data exchanges in the context of intra-European police cooperation. It would achieve all that, moreover, without posing a hindrance to effective policing at the national or European level."
>
> (D. Korff, The feasibility of a seamless system of data protection rules for the European Union, Final Report, *conclusions*)

In other words, the exclusion of certain state security- and police matters from the scope of the EC Framework Directive on data protection is the result of internal EU complexities, linked to the different legal regimes for the different "pillars" of the Union. It does not affect the need for the UK Information Commissioner to follow the general, "constitutional" approach to data protection so clearly endorsed by the European courts. On the contrary, it is generally recognised that the basic principles and criteria of the Framework Directive should be applied "seamlessly" to matters within and without the scope of Community law. In matters relating to intelligence and law enforcement, the authorities (and third parties cooperating with the authorities) can - and should - rely on the exception clauses in the Directive and the ECHR. But the use of such exception clauses should be tested with reference to the case-law of the European courts. The limited scope of the Framework Directive should not be seen as a means to evade the "constitutional"/European requirements. On the contrary, it is precisely in connection with the application of exceptions that the European principles become crucial. Any attempt to avoid those tests is likely to lead to contraventions of the ECHR - and thus also the HRA.

---

[297] *Idem*, p. 7, points 1 – 3. Parliament also demands that it "should also be consulted on, and have decision-making powers in respect of, all proposals concerning or having an impact on the protection of privacy within the EU, such as international agreements involving its bodies, adequacy findings and so on."(point 3).

4. The Legal Framework

2.3 Assessing "adequacy": a reflection of the "constitutional" approach in the assessments of data protection in third countries by the Working Party[298]

2.3.1 General

As noted by the ECJ in the cases discussed above, the EC Framework Directive on data protection seeks to ensure a common "high level" of data protection for the processing of personal data in the European Union both in order to protect the fundamental rights of the European citizens and to remove obstacles to free trade within the Union. This, in turn, requires a harmonised approach to the export of personal data from any EU Member State to any non-EU (so-called "third") country. Otherwise, the "high-level" regime of the Framework Directive could be circumvented by controllers removing personal data from the jurisdiction of the national laws implementing the Framework Directive.

The basic rule in the Framework Directive is that personal data may, in principle, only be transferred to a third country if "the third country in question ensures an adequate level of [data] protection" (Art. 25(1)), subject to certain limited derogations (exceptions) (provided for in Art. 26).[299]

The issue is of relevance to this study for two reasons. First of all, to the extent that data protection is not yet provided "seamlessly" to matters both within and without the scope of Community law, transfers of data from areas within the scope of Community law (such as, for instance, data generated as a result of commercial activities by communication- or internet service providers, airlines or retailers) to areas outside the scope of Community law (such as, typically, "Third Pillar" areas) raise a similar issue to the issue of transfers of data to third countries: the data leave an area of high protection to go to an area in which such protection may not be ensured. If data protection as a fundamental human right is not to be undermined, that should only be allowed after an assessment of whether there is "adequate" protection in the new area - such as law enforcement.

Secondly, the Working Party established by Art. 29 of the Framework Directive, which is charged with formulating an opinion of the adequacy of protection in third countries, has developed a consistent, standard approach to this issue, which reflects the "constitutional" approach to data protection developed by the European courts and described in the earlier sub-sections. We suggest that the Information Commissioner should take this approach into account in particular in any assessment of transfers of personal data from private-sector controllers to law enforcement agencies.

2.3.2 The basic approach: two elements of "adequacy"

According to Art. 25(2) of the Framework Directive:

> "The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the

---

[298] This section draws on D. Korff, Data Protection Law in the EU (footnote 1, above), Chapter 7, section iii, *The European Regime for Transfers of Personal Data to Non-EU/EEA ("Third") Countries.*

[299] The latter includes an exception allowing for transfers when "the transfer is necessary or legally required on important public interest grounds" (Art. 26(1)(d)). However, this exception must of course be read in a manner compatible with the fundamental, "constitutional" requirements we set out earlier (which flow from the ECHR and the "general principles of EC [and EU-] law").

> purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country."

The question of "adequacy" was given early attention by the Working Party established by Art. 29 of the Directive by the Directive.[300] From the beginning the Working Party felt that:

> "any meaningful analysis of adequate protection must comprise the two basic elements: the **contents** of the rules applicable, and **the means for ensuring their effective application**"[301]

This approach - requiring an analysis of both the "adequacy" of any *substantive rules* protecting the data of individuals and of the "effectiveness" of any available systems of *redress, supervision and enforcement* (including the existence of "*dissuasive sanctions*") - has been confirmed and elaborated on by the Commission and the Working Party in subsequent opinions, reports and decisions. In particular, it has been covered in the Working Party's subsequent Working Document on transfers of personal data to third countries (WP 12).[302] The European Parliament endorsed this approach explicitly in its Report on the "Safe Harbor" arrangements, concerning transfer of personal data to the USA.[303]

According to the Working Party, an "adequate" data protection system should comprise, at least:

> "a 'core' of data protection **'content' principles** and **'procedural/enforcement' requirements**, compliance with which could be seen as a minimum requirement for protection to be considered adequate. (WP 12, p. 5, emphasis added)

The Working Party continued to say:

> "Such a minimum list should not be set in stone. In some instances there will be a need to add to the list, while for others it may even be possible to reduce the list of requirements. The **degree of risk** that the transfer poses to the data subject will be an important factor in determining the precise requirements of a particular case. Despite this proviso, the compilation of a **basic list of minimum conditions** is a useful starting point for any analysis." (*idem*, emphasis added)

2.3.3 Adequacy of the substantive rules

Whether the rules meet the "contents" (i.e. substantive) requirement is to be measured by reference to the data protection principles found in Art. 6 of the Framework Directive (and in

---

300 Working Party Discussion Document WP 04 of 26 June 1997, *First Orientation on Transfers of Personal Data to Third Countries–Possible Ways Forward in Assessing Adequacy.* For related early studies in this area, see also: Y Poullet, la protection adéquate dans les flux transfrontières de données, paper presented at the 19th International Conference of Data Protection Commissioners, Brussels, September 1997, and the Commission Study, carried out by Prof. Poullet *et al.*, Preparation of a methodology for evaluating the adequacy of the level of protection of individuals with regard to the processing of personal data, Brussels, 1998.

301 Working Party Discussion Document WP 04 (see previous footnote), p. 5, emphases added. This is reflected in somewhat different terms in the "methodology" study also referred to in the previous footnote, under such headings as "risk factors", "means of protection" and "process."

302 Working Party Working Document WP 12 of 24 July 1998 on *Transfers of Personal Data to Third Countries : Applying Articles 25 and 26 of the EU Data Protection irective.* For the *verbatim* repeat of the passage quoted in the text, see p. 5.

303 European Parliament Report on the "Safe Harbor," EP Document A5- 0177/2000, of 22 June 2000.

the Council of Europe Convention, and the OECD- and UN Guidelines); the "criteria for making data processing legitimate (contained in Art. 7 of the Directive); and the provisions concerning the informing of data subjects and the rights of data subjects (in particular, Arts. 10, 11 and 12 of the Directive). The Working Party has, in effect, provided a simplified summary of the relevant substantive requirements in the form of a set of basic **"**content principles" that must be reflected in the third-country rules to be assessed:

(i) Content Principles

The basic principles to be included are the following:

1) *The purpose limitation principle*: Data should be processed for a specific purpose and subsequently used or further communicated only insofar as this is not incompatible with the purpose of the transfer. The only exemptions to this rule would be those necessary in a democratic society on one of the grounds listed in Article 13 of the Directive.

2) *The data quality and proportionality principle***:** Data should be accurate and, where necessary, kept up to date. The data should be adequate, relevant and not excessive in relation to the purposes for which they are transferred or further processed.

3) *The transparency principle***:** Individuals should be provided with information as to the purpose of the processing and the identity of the data controller in the third country, and other information insofar as this is necessary to ensure fairness. The only exemptions permitted should be in line with Articles 11(2)3 and 13 of the Directive.

4) *The security principle***:** Technical and organisational security measures should be taken by the data controller that are appropriate to the risks presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process data except on instructions from the controller.

5) *the rights of access, rectification and opposition***:** The data subject should have a right to obtain a copy of all data relating to him/her that are processed, and a right to rectification of those data where they are shown to be inaccurate. In certain situations he/she should also be able to object to the processing of the data relating to him/her. The only exemptions to these rights should be in line with Article 13 of the Directive.

To this is added a further "basic principle":

6) *Restrictions on onward transfers***:** Further transfers of the personal data by the recipient of the original data transfer should be permitted only where the second recipient (i.e. the recipient of the onward transfer) is also subject to rules affording an adequate level of protection. The only exceptions permitted should be in line with Article 26(1) of the Directive.

(WP 12, p. 6, original emphasis)

However, according to the Working Party, there will be a need for "additional principles" in certain circumstances. The Working Document provides three examples of such additional principles, the first and third of which are relevant to this study:[304]

---

[304] The second issue for which additional principles are required is *direct marketing*. In that respect, the document says: "Where data are transferred for the purposes of direct marketing, the data subject should be able to 'opt-out' from having his/her data used for such purposes at any stage." (point 2).

"*sensitive data*: Where 'sensitive' categories of data are involved (those listed in article 8 of the Directive), additional safeguards should be in place, such as a requirement that the data subject gives his/her explicit consent for the processing.

...

automated individual decision: Where the purpose of the transfer is the taking of an automated decision in the sense of Article 15 of the Directive, the individual should have the right to know the logic involved in this decision, and other measures should be taken to safeguard the individual's legitimate interest."

(WP 12, p. 7, points 1 and 3, numbering omitted, original emphasis)

2.3.4 Effectiveness of the supervisory and enforcement system

On the question of the "adequacy" of the available system of *supervision and enforcement*, the Working Party has the following to say:

(ii) Procedural / Enforcement Mechanisms

In Europe there is broad agreement that data protection principles should be embodied in law. There is also broad agreement that a system of 'external supervision' in the form of an independent authority is a necessary feature of a data protection compliance system. It is not sufficient, however, to simply state, without any form of reasoning or justification, that these two features are in some way inherently necessary for the protection to be adequate. To do so would be to draw up purely formalistic criteria for evaluating this question.

It is suggested that a better starting point is to seek to identify the underlying objectives of a data protection procedural system, and on this basis to judge the variety of different judicial and non-judicial procedural mechanisms used in third countries in terms of their ability to meet these objectives.

The objectives of a data protection system are essentially threefold:

1) To deliver a *good level of compliance* with the rules. (No system can guarantee 100% compliance, but some are better than others). A good system is generally characterised by a high degree of awareness among data controllers of their obligations, and among data subjects of their rights and the means of enforcing them. The existence of effective and dissuasive sanctions is important in ensuring respect for rules, as of course are systems of direct verification by authorities, auditors, or independent data protection officials.

2) To provide *support and help to individual data subjects* in the exercise of their rights. ..The individual must be able to enforce his/her rights rapidly and effectively, and without prohibitive cost. To do so there must be some sort of institutional mechanism allowing independent investigation of complaints.

3) To provide *appropriate redress* to the injured party where rules are not complied with. This is a key element which must involve a system of independent arbitration which allows compensation to be paid and sanctions imposed where appropriate.

(WP 12, p. 7, original emphasis)

2.3.5 Taking into account of specific risks

As already noted, according to the Working Party, the degree of *risk* that the transfer poses to the data subject will be a further important factor in determining the precise requirements of each case. The Working Party already included a list of "categories of transfers which it considers pose particular risks to privacy" in its initial Discussion Document (WP 04).[305] They are:

- transfers involving certain *sensitive categories of data* as defined by Article 8 of the Directive;
- transfers which carry the *risk of financial loss* (e.g., credit card payments over the Internet);
- transfers carrying a *risk to personal safety*;
- transfers made for the purposes of making *a decision which significantly affects the individual* (such as recruitment or promotion decisions, the granting of credit, etc.);
- transfers which carry *a risk of serious embarrassment or tarnishing of an individual's reputation*;
- transfers which may result in specific actions which constitute *a significant intrusion into an individual's private life*, such as unsolicited telephone calls;
- repetitive transfers involving *massive volumes of data* (such as transactional data processed over telecommunications networks, the Internet, etc.);
- transfers involving the collection of data in *a particularly covert or clandestine manner* (e.g., Internet cookies).

(WP 4, pp. 4 – 5, emphasis added)

The Working Party said that it intended to produce a "specific and more detailed paper outlining the categories of transfer which it considers pose particular risks to privacy" (*idem*, p. 4), but it has not yet done so. However, it included the same list of "transfers posing specific risks" in its subsequent Working Paper (WP 12). In that paper it said that if a specific role is given by the Member States to the supervisory authority either to authorise data transfers before they take place or to carry out an *ex post facto* check, the list "would constitute guidance regarding which cases of data transfer should be considered as 'priority cases' for examination or even investigation" by those data protection authorities.

2.3.6 Similar assessments

In WP12 (discussed above), the Working Party also briefly examined the question of whether the **Council of Europe Convention on data protection** accorded "adequate" protection, by reference to the "check-list" of issues set out above. It concluded that while the Data Protection Convention provided "adequate" protection in respect of most of the "content" principles, it failed to prohibit transfers to countries without "adequate" protection, and did not sufficiently provide for supervision and enforcement:

---

305 For a more abstract "risk analysis table", see the "methodology" study (footnote 73, above), p. 7ff.

> "As regards the content of the basic principles, the Convention could be said to include the first five of the six 'minimum conditions'. The Convention also includes the requirement for appropriate safeguards for sensitive data which should be a requirement for adequacy whenever such data are involved.
>
> A missing element of the Convention in terms of the content of its substantive rules is the absence of restrictions on transfers to countries not party to it. This creates the risk that a Convention 108 country could be used as a 'staging post' in a data transfer from the Community to a further third country with entirely inadequate protection levels.
>
> The second aspect of 'adequate protection' concerns the procedural mechanisms in place to ensure that the basic principles are rendered effective. The Convention requires its principles to be embodied in domestic law and that appropriate sanctions and remedies for violations of these principles are established. This should be sufficient to ensure a reasonable level of compliance with the rules and appropriate redress to data subjects where the rules are not complied with (objectives (1) and (3) of a data protection compliance system). However, the Convention does not oblige contracting parties to establish institutional mechanisms allowing the independent investigation of complaints, although in practice ratifying countries have generally done so. This is a weakness in that without such institutional mechanisms appropriate support and help to individual data subjects in the exercise of their rights (objective (2)) may not be guaranteed."
>
> (WP 12, Chapter Two, p. 9)

To this, the Working Party added in a footnote:

> "There may be some doubts about the 'transparency principle'. Article 8 (a) of the Convention may not equate to the *active* duty to provide information which is the essence of Articles 10 and 11 of the directive. Furthermore the Convention includes no specific 'opt-out' rights where data are used for direct marketing purposes nor any provisions on automated individual decisions (profiling)."

Since the above criticisms were made, an additional protocol to Convention No. 108 has been drafted, which adds two substantive new provisions to the convention, one on the setting up of one or more supervisory authorities by each Party and one on transborder flows of personal data to countries or organisations that are not parties to the Convention.[306] The protocol was adopted on 23 May 2001 and opened for signature on 8 November of that year. However, the protocol has not yet received the required five signatures to enter into force. That, however, is a side issue in the present context. What we wish to note here is the reiteration, by the Working Party, of its standard approach to "adequacy"; we merely wish to show how serious the Working Party takes compliance with all its tests, even with regard to States that are a Party to the Data Protection Convention (which is, in a way, one of the parents of the Framework Directive itself).

The same can be said with regard to the Working Party's detailed assessment of the so-called "**Safe Harbor**" arrangements, under which personal data can be transferred from the EU to companies that have "self-certified" that they will comply with the principles and procedures

306 Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding Supervisory Authorities and Transborder Data Flows, ETS 181.

set out in those arrangements. The matter is too complex to discuss in detail here.[307] But it may be noted that in that context, too, the Working Party closely examined whether the arrangement: (a) ensured compliance with the basic data protection principles; (b) prohibited onward transfers of the data to countries or controllers which do not guarantee continued "adequate" protection; (c) provided for adequate openness, both in general and in terms of information provided to data subjects; (d) established a clear enforcement mechanisms (subject to ultimate State control); and (e) granted full, and enforceable, data subject rights.

Under the Framework Directive, assessments of the "adequacy" of protection in a third country can relate to certain sectors or controllers (thus, the "Safe Harbor" arrangement only applies to controllers in the USA who have decided to join the arrangement). In spite of he reference to domestic law in Art. 25(6) of the Directive, the Working Party is prepared to also examine **self-regulatory codes of conduct** in this regard, provided they are embedded in the legal system in question in such a way as to ensure that the rules in the codes can be effectively relied on by data subjects and if needs be enforced by the State.[308]

In the Working Party view, the assessment of the "content" of a code, i.e., of its substantive adequacy, is "a relatively easy task": it is basically a question of ensuring that the necessary "content principles" are contained in the code; this merely requires an "objective evaluation." (WP 12, p. 11)

The strong emphasis of the Working Party's assessment of the adequacy of self-regulation is therefore on *enforcement*. The Working Party stresses that "the three functional criteria for judging the effectiveness of protection" - a good level of compliance; support and help to individual data subjects; and appropriate redress - must all be met if a self-regulatory code is to be considered as providing adequate protection (*idem*). The Working Party demands, in particular, a strong system of sanctions against companies which violate a code:

> The absence of **genuinely dissuasive and punitive sanctions** is therefore a major weakness in a code. Without such sanctions it is difficult to see how a good level of overall compliance could be achieved. ... (WP 12, p. 12)

If a sector (i.e., a sectoral association responsible for a code) does not itself provide for such "punitive sanctions", there must be "a rigorous system of *external* verification." This means that there must be:

> "[either] a public or private authority competent to intervene in case of non compliance with the code, or a compulsory requirement for external audit at regular intervals."

It is furthermore clear from the Working Party's observations (phrased in the form of questions expressing matters to be taken into account) that there should be "a *system* in place allowing for investigation of *complaints* from individual data subjects"; the data subjects should be made *aware* of this system and of the *decisions* taken in individual cases; *investigations* should be carried out by *independent and impartial arbiters or adjudicators*, and the latter should have "the necessary *powers*" to conduct such investigations (cf. WP 12, p. 12):

---

307 For a detailed discussion, see D. Korff, Data Protection Law in the EU (footnote 1, above), Chapter 7, section iv, *applying the new European regime to transfers of personal data from the EU to the USA: the "Safe Harbor" arrangements.*

308 See D. Korff, Data Protection Law in the EU (footnote 1, above), Chapter 7, section iii, sub-section (b), under the heading "*providing adequate protection through sectoral (self-) regulation*".

> "Ideally the arbiter should also come from outside the profession or sector concerned, the reason being that fellow members of a profession or sector have a clear commonality of interests with the data controller alleged to have breached the code. Failing this the neutrality of the adjudicating body could be ensured by including consumer representatives (in equal numbers) alongside the industry representatives."

Sanctions that are able to *remedy* a breach of the rules must be available. This means that the above-mentioned "arbitrators or adjudicators" must be able to demand remedial action, and that the taking of that remedial action can be *verified*. Individuals whose rights or interests have been damaged should furthermore be able to obtain *compensation* under the code. The latter in particular again suggest that there should be at least a link with the domestic legal system: the Working Party document asks, in particular:

> "is the breach of the code equivalent to a breach of contract, or enforceable under public law (e.g. consumer protection, unfair competition), and can the competent jurisdiction award damages on this basis?" (WP 12, p. 12)

The Working Party sums up its *conclusions* concerning self-regulation as follows:

- Self-regulation should be evaluated using the objective and functional approach set out in Chapter One. [i.e., it should contain both the 'core' of data protection 'content' principles and the 'procedural/enforcement' requirements as summarised previously.]

- For a self-regulatory instrument to be considered as a valid ingredient of "adequate protection," it must be binding on all the members [of the trade association responsible for the code] to whom personal data are transferred and provide for adequate safeguards if data are passed on to non-members;

- The instrument must be transparent and include the basic content of all core data protection principles;

- The instrument must have mechanisms which effectively ensure a good level of general compliance. A system of dissuasive and punitive sanctions is one way of achieving this. Mandatory external audits are another;

- The instrument must provide support and help to individual data subjects who are faced with a problem involving the processing of their personal data. An easily accessible, impartial and independent body to hear complaints from data subjects and adjudicate on breaches of the code must therefore be in place.

- The instrument must guarantee appropriate redress in cases of non-compliance. A data subject must be able to obtain a remedy for his/her problem and compensation as appropriate.

The Working Party has applied the same tests to **standard data transfer contracts** and **intra-corporate data protection arrangements**; and in its own **standard European data transfer contract clauses**.[309]

We suggest that the Information Commissioner should apply these same tests with regard to any transfers, by private- or public-sector bodies to law enforcement agencies.

---

309 See D. Korff, Data Protection Law in the EU (footnote 1, above), Chapter 7, section iii, sub-section (d), under the corresponding headings.

We also submit that the above confirms the general, "constitutional" approach to data protection; that the above principles and tests are of a nature to be applied, and are intended to be applied, to *any* serious data protection issue. They can - and should - be drawn upon in the Information Commissioner's approach, also to privacy and law enforcement.

3. Adopting the "constitutional" approach to data protection with regard to data processing for law enforcement purposes

3.1 "Policing" - a complex concept[310]

Before discussing the "constitutional"/European-legal approach to data protection and law enforcement, it should be noted that the concepts of "police" and "policing" are not straight-forward. As Boldt put it in his historical description of the police in Germany:

> "The lack of clarity [in defining the concept and role of the police], which fundamentally persists to this day, is a result of the fact that the police is the product of a historical development and not of a rational construction of state administration."[311]

This lack of clarity even about the basic tasks and purposes of police work (and of the processing of personal data in the course of that work) has a direct impact on the question of the application of data protection rules and -principles, since these crucially hinge on the core concept of "purpose-specification" and "-limitation".

The confusion extends to the Council of Europe Recommendation *Regulating the Use of Personal Data in the Police Sector*, further discussed below, at 3.3, which initially defines "police purposes" as:

> "all the tasks which the police authorities must perform for the prevention and suppression of criminal offences and the maintenance of public order." (Scope and Definitions)

However, as the Explanatory Memorandum to the Recommendation makes clear, this rather broad statement of the overall police task must be refined when it comes to the application of specific provisions:

> "so as to ensure that the principles will treat differently the tasks which the police must perform in regard to the suppression of criminal offences and the tasks which it must carry out at the level of prevention and the maintenance of public order." (Explanatory Memorandum, para. 22)

Consequently, the first substantive principle in the Recommendation, Principle 2.1, already distinguishes between the collection of personal data "***for the prevention of a real danger***" and the collection of such data "***for the suppression of a specific criminal offence***" - while allowing for the possibility that domestic law "clearly authorises wider powers to gather information". In various other paragraphs (e.g., paras. 8 and 21), the Explanatory

---

310 This section largely repeats (with some minor changes) the sub-section on "*police purposes and activities*" (sub-section 1 of section IV.C) in D. Korff, The feasibility of a seamless system of data protection rules for the European Union (above, footnote 1).

311 Hans Boldt, *Geschichte der Polizei in Deutschland*, in: Lisken\Denninger (Eds.), Handbuch des Polizeirechts, 2nd. Ed., Munich, 1996.

Memorandum similarly notes the distinction between "the classic and crucial tasks of the police" and "particular requirements, notably in respect of the 'suppression [read: prevention] of criminal offences'". The Recommendation also stresses that the use of personal data by the police for purposes which are not strictly police purposes (such as administrative purposes) must comply with the general data protection principles: such processing does not benefit from the special exceptions granted in respect of processing for police tasks.

The Recommendation is therefore not entirely clear as to what tasks exactly are carried out by the police - but acknowledges that there is a trend to extend the tasks of the police beyond the "classic tasks".

This is confirmed by the situation in the Member States, in all of which the tasks and functions of the police (and even the concept of "the police" itself) are somewhat ill-defined and changing. Partly this has historical reasons: over the centuries, the concept of "police" has evolved (at least on the Continent) from referring quite generally to the advancement of state policy to a more limited concept focusing on law enforcement. In the modern era, the "classic tasks" of the police in a democratic society have come to be defined as:

Ÿ **the investigation and prosecution of specific criminal offences**; and

Ÿ **the countering of (real and immediate) threats to public order**.

However, from at least the 1970s onward, the presumed general increase in criminality - but more in particular the new threats to society posed by drugs-related and other organised crime, and especially by terrorism, led to a very significant extension of the role of the police into a further, previously much more marginal area:

Ÿ **prevention** [of criminal offences being committed, or of threats to public order materialising - the distinction is not always clear].[312]

"Preventive" police work, in practice, means the collecting, storing and analysing of so-called "**intelligence**" information on individuals who *might* commit (certain) crimes, or who operate in certain (targeted) circles. The notable trend towards more and more "preventive" policing in the Member States shows remarkably similar - and some would say, disturbing - features:

- it involves the collecting of personal data on a **wider range of data subject**: i.e. not just on persons (reasonably) suspected of involvement in a criminal offence, or who pose a clear and immediate threat to public order (the targets of "classic" policing), but also on persons who "*might*" be involved in, or who "*might become*" involved in, (certain, not always very-well-defined types of) "serious" crime or disturbances and indeed on people who are "*in contact with*" such already ill-defined targets;

- it involves the increased use of **more intrusive, secret means of data collection** (telephone tapping, "bugging" of homes and offices, the use of informers and undercover agents, etc.) against this wider range of objects of police enquiries;

---

312 In France, the special police department of the *Renseignements Generaux* has, since the time of the German occupation, been responsible for general information-gathering on persons of public interest, for no other reason than to keep the Government informed (i.e. neither to prevent crime nor to counter any direct threat nor indeed for "prevention"). It is therefore doubtful whether the R-G actually serve a "police" purpose.

- it involves **more intrusive means of data processing** including, in particular, ever-wider **"data matching"** including the special police technique of ***Rasterfahndung***: the screening of various (not necessarily only police- or public sector-) databases against pre-determined criteria, to "filter out" from a *general population*, individuals who are deemed to merit further police attention of the above kind; and

- it involves **an increased blurring of the distinction between the work of the police and the work of the intelligence services**.

These changes in the police's brief and operational environment also affect institutional aspects of policing. Tradionally, in most Member States, policing is largely, or at least partly, decentralised: e.g., in the UK, to 43 local police forces; in the Netherlands to 25 regional forces; and in Germany, to the *Laender*; in others (e.g. France, Italy) there have always been strong, central (often militarised) police forces, but even there combined with local police units. While there have aways been central institutions to coordinate and support the regional forces (e.g., in the UK, the Home Office and the *primus inter pares* force, the Metropolitan Police which includes Scotland Yard; in the Netherlands, the CRI - now DCRI; and in Germany, the BKA), the above-mentioned changes in police focus and operational methods have greatly increased the role and status of such institutions; many have been reformed to adapt to their new role, or additional institutions (e.g., in the UK, NCIS) have been set up. In particular, these central institutions tend to be responsible for the most important "criminal intelligence" databases and data processing operations; and they increasingly "guide" (rather than merely "support") the work of the regional forces - again especially in the new, "preventive" area of police work.

Finally, the internationalisation of crime - and in particular of organised crime and of terrorism - has led to a corresponding internationalisation of policing. All the EU Member States have established special units (often expanded from or otherwise incorporating the Interpol NCBs) to deal with the greatly increased, and increasing, internationalisation of policing - also and in particular in a European (i.e. Europol) context. These units, too, tend to be established at a central level - often within the same institutions as the central databases - and internationalisation has therefore reinforced centralisation of policing at the national level.

In sum: *in all the EU Member States there has been, over the last twenty years, a significant expansion of police work into the area of "preventive" (and mostly secret) "intelligence"-gathering, also and in particular on persons who would not previously have been the object of police investigations; and this expansion has coincided with increased centralisation - especially in the field of computer analysis - and internationalistion.* ***Policing in Europe at the end of the 20th and the beginning of the 21st century is more sophisticated, more intrusive, more secret, and more centralised than ever since the Second World War.***

These developments have a serious impact on human rights and civil liberties, and more generally on the relationship between the individual and the State. They raise important, and sometimes disturbing questions of legitimacy, democracy and constitutionality; as Prof. Simitis, the *eminence grise* of European data protection, has observed.

> "only the greatest possible transparency under the rule of law, also of police activities, ensures that the danger of slipping into a surveillance state can be countered."[313]

These changes in the work of the police - and most notably the above-mentioned fundamental changes in the collection, storing, analysing and use (in short: in the processing) of personal data, and the changed purposes of that processing - affect the way in which the data protection principles are applied (or should be applied) to the police. In our view, they greatly underscore the need for a strong, "constitutional" approach to data protection and law enforcement. More in particular, we submit that in applying the "purpose-limitation" principle, the Information Commissioner should distinguish between the different "police" purposes, as is done in other countries, as discussed next.

3.2 The approach to the processing of personal data for law enforcement purposes in countries in which data protection has a constitutional basis

In this sub-section, we will try to set out briefly, and in general terms, the approach to the processing of personal data for law enforcement purposes in a number of countries in which data protection has a constitutional basis: Germany, France, Italy and the Netherlands. The aim is merely to illustrate the general approach in such countries. In the next section, we will show how the same approach is taken in the Council of Europe Recommendation *regulating the use of personal data in the police sector* (Recommendation R(87)15). To give an insight into the more detailed thinking on these matters, a paper is attached on the country with perhaps the strongest constitutional framework in this respect, Germany[314] (in the final paper, we will show the way in which certain selected issues are looked at from the European point of view and from the similar constitutional perspective described in this section.)

In the above-mentioned countries, the fact that data protection has a constitutional basis means that the collection, storing and use (i.e. the processing) of personal data by the police must be "**necessary**" to serve the police task - or rather, ***a*** (specific) police task (see below). Specifically, personal data should never be collected by the police or other law enforcement agencies "***just in case***".[315] It also means that exceptions to more specific data protection requirements - such as purpose-limitation, the duty to inform data subjects of processing of their data, or the granting of subject access - must also be "**necessary**" in this sense.

This stricter approach is reinforced by the more precise definition, in countries with a "constitutional" approach, of the various "police purpose**s**". In the UK, the legal rules (and the rules in the ACPO Code) are built around a concept of "the police task" which encompasses all aspects of policing: "the prevention and detection of crime: apprehension and prosecution of offenders: maintenance of law and order, and rendering assistance to the public". Data obtained for any of these purposes can be freely used for any other of these purposes when "relevant"; this even applies to data provided by data subjects in the course of an access request. By contrast, the other legal systems require that the various tasks of the police be more clearly distinguished and separated and that the data protection rules and principles - and the "necessity" tests mentioned above - be applied accordingly.

---

313 13th Annual Report of the Data Protection Commissioner for the *Land* Hessen (1984), p. 34.

314 See Annex 2. Both this sub-section and that annex again draw on D. Korff, The feasibility of a seamless system of data protection rules for the European Union, 1997.

315 What the Germans call, "*auf Vorrat*". Cf. the emphatic re-affirmation of this principle by the German Data Protection Authorities with regard to the European proposals to require communication service providers and ISPs to retain communication- and "browsing" information, quoted in Annex 2.

Thus, in Germany, the very extension of the work of the police beyond the "classic" tasks of investigation and prosecution of criminal offences and the countering of threats to public order must be assessed under the "necessity" test: "preventive" policing can, in that country, only ever be "necessary" (and hence, compatible with the Constitution) in respect of (specifically listed) "serious offences"; and the same applies, e.g., to the collection of data on "contacts and associates" (i.e. on persons not suspected of involvement in a specific crime or of posing a threat), to the collection of information through intrusive, secret means ('phone tapping; "bugging"; informers; agents), and to the use of *Rasterfahndung* ("profiling"). The use of personal data, collected for one specific police purpose (e.g. countering threats) can, moreover, only be used for another specific purpose (e.g. investigating offences) if the data could have been independently collected for that second purpose.

The constitutional approach also requires **as much openness as possible** about police data processing, and especially about the use of secret police measures such as telephone- and other communications interception or –monitoring, undercover surveillance, the use of informers and infiltrators, etc.[316]

In these countries, it is also a constitutional requirement that individuals have an **effective remedy** against alleged violations of these principles: the question of whether interferences with fundamental rights are based on such rules, and whether the rules (and the application of these rules) conform to the principle of "necessity" must, in these countries, in principe always, ultimately be ***justiciable***. It follows from the constitutional principles of "necessity" and "proportionality" that only the most exceptional circumstances can justify alternative, non-judicial remedies. In all cases, there must at least be **close supervision** by an ***independent and impartial authority*** - either the national data protection authority or a special authority with no less independence.

This approach of course corresponds to the approach taken by the European Court of Human Rights and the European Court of Justice under the ECHR and "general principles of law", as discussed above, at 2.2.

The implications of the basic, constitutional approach to such matters are well set out in two sets of guidelines, drawn up by the Conference of German Data Protection Authorities as long ago as 1985, and attached to this paper as Annex 3. They are the:

- Data Protection Requirements for the Police; and the
- Data Protection Requirements for the Intelligence Service.[317]

---

316 Cf., for another good German example of the general approach: Entschließung der 48. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27.09.1994 - *Vorschläge zur Überprüfung der Erforderlichkeit polizeilicher Befugnisse und deren Auswirkungen für die Rechte der Betroffenen* (Decision of the 48th Conference of Data Protection Authorities of the Federation and of the States of 26/27.09.1994 – *Recommendations concerning the supervision of the necessity of special police powers and their effect on the rights of data subjects*). Note in particular also the recent Entschließung der 66. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 25./26. September 2003 in Leipzig - *Konsequenzen aus der Untersuchung des Max-Planck-Instituts über Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation* (Decision of the 66th Conference of Data Protection Authorities of the Federation and of the States of 25/26 September 2003 – *Implications of the study of the Max Planck Institute into the legal reality and effectivity of telecommunications surveillance*), which provides detailed statistical information on communication interception orders, obtained in a study by the Max Planck Institute for comparative and international criminal law, and draws detailed conclusions from these statistics.

317 Respectively: Anforderungen an Datenschutzregelungen im Polizeirecht (24 January 1985);

In the countries mentioned, such mere guidelines are, however, not sufficient. Rather, it follows from the fact that data protection has a constitutional basis that, in the countries in question, police data processing must be regulated in **specific, detailed legal rules** relating to **specific operations or databases**, for **specific police tasks**. These rules should clarify how compliance with the basis principles is to be ensured for such operations and tasks.[318] Thus, in France, each police data processing operation must be based on a governmental regulation (*acte réglementaire*) adopted after the data protection authority has given its opinion on the regulation. In Italy, the recent (2003) Data Protection Code (which consolidates earlier data protection laws and –rules) similarly stipulates:

Section 57
(*Implementing Provisions*)

1. A Presidential Decree issued following a resolution by the Council of Ministers, acting on a proposal put forward by the Minister for Home Affairs in agreement with the Minister of Justice, shall set out the provisions implementing the principles referred to in this Code with regard to data processing operations performed by the Data Processing Centre [a centralised police centre – DK] as well as by police bodies, offices and headquarters for the purposes mentioned in Section 53, also with a view to supplementing and amending Presidential Decree no. 378 of 3 May 1982, and by putting into practice Council of Europe's Recommendation No. R(87)15 of 17 September 1987 as subsequently modified. Said provisions shall be set out by having regard, in particular, to:

a) the principle by which data collection should be related to the specific purpose sought, in connection with preventing a concrete danger or suppressing offences, in particular as regards processing operations for analysis purposes,

b) regular updating of the data, also in connection with assessment operations carried out under the law, the different arrangements applying to data that are processed without electronic means and the mechanisms to notify the updated information to the other bodies and offices that had previously received the original data,

c) the prerequisites to carry out processing operations on transient grounds or else in connection with specific circumstances, also with a view to verifying data quality requirements as per Section 11, identifying data subject categories and keeping such data separate from other data for which they are not required,

d) setting out specific data retention periods in connection with nature of the data or the means used for processing such data as well as with the type of proceeding in whose respect they are to be processed or the relevant measures are to be taken,

e) communication of the data to other entities, also abroad, or else with a view to exercising a right or a legitimate interest, as well as to dissemination of the data, where this is necessary under the law,

f) use of specific data processing and retrieval techniques, also by means of reverse search systems.

---

and Anforderungen an Datenschutzregelungen für den Verfassungsschutz (13 September 1985).

318 In Germany and Italy, it is also a constitutional requirement that the primary rules allowing for such departures from the normal constitutional (*in casu*, data protection) guarantees must be set out in a formal statute (even if the detailed application of the exceptions can be further regulated in lower-level, subsidiary rules). In Germany, this is referred to as *Gesetzesvorbehalt*.

In the same vein, the recent German Federal Law on the Federal Bureau for Criminal Matters (BKA), which itself already contains quite elaborate data protection principles, requires the following:

> **§ 34**
> *Orders for the establishment [of automated personal data filing systems]*
>
> (1) The Federal Bureau for Criminal Matters must specify, for each automated personal data filing system maintained by it for the fulfilment of its tasks, in an order which requires the approval of the Federal Ministry of the Interior, the following matters:
>
> 1. the name of the filing system;
> 2. the legal basis and [specific] purpose of the system;
> 3. the kinds of people about whom data are to be held [in the system];
> 4. the kinds of personal data that are to be held [in the system];
> 5. the kinds of personal data which serve to access the system;
> 6. the manner in which the data are obtained or entered;
> 7. the conditions under which the data in the system are passed on to which recipient and subject to which procedure;
> 8. the intervals at which the data must be verified and the maximum retention period;
> 9. the manner in which records are to be kept.
>
> The Federal Data Protection Authority must be asked for his opinion [on each such order] before the order is issued.

The Dutch Police Data Protection Law similarly stipulates a "double necessity" test for police data processing, coupled with a requirement for further regulation: no personal data filing system may be established for police purposes, unless this is "necessary" for the specific purpose in question; the data in any such system must furthermore also be "necessary" for that purpose; and this must be clarified, for specific police filing systems, in specific regulations.

Neither the Italian decree nor these specific German orders have as yet been adopted; in both countries, such processing is for the moment based on earlier rules (which do not always meet the constitutional requirements). However, in the Netherlands, a large number of detailed regulations have been adopted which formally limit what data can be collected and stored on what types of data subject in which database or "register". There are, to date, some 40 such regulations, each covering one such register.[319] Thus, on witnesses, only name, address, date of birth, nationality, and information on the offence may be recorded, while on (formal) suspects, information on (*inter alia*) profession, appearance (including photographs), fingerprints etc. can be held. If the suspect is a "CID-subject" (i.e. suspected of involvement in "serious crime"), much more sensitive "intelligence" information, on lifestyle, character etc. can be kept; etc. But no such data can be kept on persons suspected of involvement in lesser offences. The basic idea is clearly to limit the information held to what can be said to be "necessary" and "proportionate" in relation to the serious nature of the matters under investigation: the holding of (say) lifestyle data on persons not suspected of a criminal offence, and indeed on "ordinary" (non-"CID") suspects is clearly regarded as disproportionate and unnecessary, and therefore disallowed. Certain detailed regulations on various police files and -databases in France and Germany are supposed to contain similar

319 See the Dutch Data Protection Authority's website: http://www.cbpweb.nl/structuur/pag_wetten.htm.

restrictions, relating the amount and nature of data stored to the nature of the police purpose concerned - but these regulations are, for the time being, kept secret (contrary to the ECHR and indeed the national constitutional requirements in these countries).

In the countries examined, the data protection autorities see it as a crucial task to seek compliance with the constitutional principles underpinning data protection: they will issue opinions on draft laws (or comment most critically on the absence of adequate, sufficiently detailed and constitution-compliant legal rules), or on practices under such laws (or which may have developed outside, or contrary to, the law), in which they will stress any constitutional defects they perceive. And they closely relate to the work of the courts in these countries, either by bringing test cases, or by being asked to give their opinion by the courts, or by providing such opinions unasked-for.

3.3 European-legal rules on the processing of personal data for law enforcement purposes

In the previous section (section 2), we have tried to show what it means to adopt a "constitutional" approach to the processing of personal data. We have shown that the European courts, as well as the Working Party, follow a clear line of reasoning in this respect: one can apply the "constitutional" (ECHR-/"general principles"-based, and WP-confirmed) approach by going through a "**check-list**" of tests, developed by the European Court of Human Rights in particular. The cases discussed show the results of this approach.

Several of the Strasbourg cases already touched on law enforcement-related issues in the broadest sense: the use of secret files for state security purposes (Leander, Amann, Rotaru); CCTV surveillance (Peck). These cases are important because they represent binding international-legal rulings from which the State-Parties to the ECHR (including the UK) may not depart - and which the Information Commissioner therefore should follow in his assessment-, guidance- and enforcement-activities.

However, they are by their nature limited by the specific facts, and by the fact that they are, of course, based only on the Convention and in particular on Art. 8 ECHR which (as we have seen) is not-too-easy a basis for data protection issues (although the Court does nowadays expressly refer to the Data Protection Convention as indicating the principles to be followed).

The wider implications of the "constitutional"/European approach for the police have been clarified in a number of more general international instruments and documents. As such, they are generally not binding in international law. However, they are the most considered views of the matters covered, by the leading expert bodies in Europe.

In our final paper, we will discuss specific opinions and recommendations on a number of selected issues in this field, issued by the Council of Europe, the Working Party established under the EC Framework Directive on data protection, and by the EU Council, with reference to national rules or guidelines reflecting the same "constitutional" approach to those issues.

Here, we want to note Recommendation No. R(87)15 of the Committee of Ministers of the Council of Europe *regulating the use of personal data in the police sector*, adopted on 17 September 1987, together with an Explanatory Memorandum clarifying the application of the set of principles appended to the recommendation. This recommendation has become the effective standard on the issue: it is referred to in various European police co-operation

instruments, including the Schengen- and Europol-treaties and associated regulations, and is also regularly invoked in recommendations by the Parliamentary Assembly of the Council of Europe and its Committee of Ministers, by the Working Party, and the European Parliament. Within the EU, the Recommendation is seen as closely linked to the so-called "soft *acquis*"of the Union in the field of police cooperation.[320] We have also already noted that the provision in the Italian Data Protection Code requiring the adoption of special decrees for police data processing (Section 57, quoted in section 3.2, above) expressly requires such decrees to comply with this recommendation.

The full texts of the Recommendation and of the Explanatory Memorandum are attached as Annex 1. Here, it may suffice to note the principles contained in the Recommendation, and the comments on them in the Explanatory Memorandum, which are of most immediate interest to the present study in the light of our earlier papers on trends in policing;[321] the Information Commissioner will note the close correspondence between these principles and the national-constitutional principles discussed in the previous sub-section.

On a preliminary issue, it may be noted, first of all, that:

> "For the purposes of this Recommendation, the expression '**personal data**' covers any information relating to an identified or identifiable individual. An individual shall not be regarded as 'identifiable' if identification requires an unreasonable amount of time, cost and manpower." (preliminary section on "scope and definitions", emphasis added)

With current technology, the retrieval of most data which are in one way or another linked to an identified or identifiable individual will, of course, rarely require an "unreasonable amount of time, cost and manpower" - in fact, as we have shown in our earlier papers, the whole thrust of modern policing is towards ever-greater ease of data finding and –matching. The point to be emphasised here is that the Recommendation clearly does not envisage a limitation of the kind invented by the Court of Appeal in Durant. The extent to which the data intrude on a person's "private life" is *irrelevant*: if the data can be retrieved by reference to the person (even if this is by means of, say, face recognition rather than name or file number) without undue effort, the data are "personal", and the rules apply.

The Recommendation also stipulates, in the same preliminary section on "scope and definitions" that:

> "The expression 'for **police purposes**' covers all the tasks which the police authorities must perform for the prevention and suppression of criminal offences and the maintenance of public order." (emphasis added)

However, the Explanatory Memorandum stresses that in the specific rules that follow, the Recommendation differentiates between the different, **more specific police purposes** that can be discerned within this broad concept, as discussed above:

---

320 See: Europa – Justice and Home Affairs – Acquis of the European Union under Title IV to the TEC and Title VI of the TEU, section VIII, *police cooperation*, at C, Other European Union Instruments (soft acquis and useful documents): http://europa.eu.int/comm/justice_home/doc_centre/police/acquis/wai/doc_police_acquis_en.htm

321 In line with the Council of Europe Convention on data protection to which it relates, the Recommendation is limited to *automated* processing of personal data. With increased (now almost ubiquitous) use of computers, also by the police, this limitation is of course becoming less and less important. Because of this, and because we are focussing on the constitutional principles reflected in the Recommendation and some selected issues rather than all its detail, this limitation is not further taken into account in this summary. See however paras. 26 and 27 of the Explanatory Memorandum to the Recommendation.

> "The principles are intended to regulate all the crucial stages where data protection becomes an issue - collection, storage, use and communication of personal data. It will be noted that these activities are linked to the finality of 'police purposes'. The latter term is defined in the light of the interests at stake for society, already referred to in the fifth paragraph of the preamble. However, it will be recalled that this statement of finality will be the subject of refinement at later stages in the text so as to ensure that the principles will treat differently the tasks which the police must perform in regard to the suppression of criminal offences and the tasks which it must carry out at the level of prevention and the maintenance of public order."
>
> (para. 22)

The Recommendation accordingly stipulates, first of all (in Principle 2.1), that the *collection* of personal data should (in principle) be limited to such as is **necessary for the prevention of a real danger** or **the suppression of a specific criminal offence** - i.e. for one of the two "classic" police tasks. Any exception to this - read: any collecting of personal data for wider, more generally "preventive"/"intelligence" purposes must the subject of "**specific national legislation**." In fact, even then, indiscriminate, "just in case", collection of data should not be allowed:

> "*Principle 2.1* excludes an open-ended, indiscriminate collection of data by the police. It expresses a qualitative and quantitative approach to Article 5.c of the Data Protection Convention which stipulates that personal data must be adequate, relevant and not excessive in relation to the purposes for which they are stored. Given that Article 9.a of the convention allows a derogation from this principle in regard to the 'suppression of criminal offences', Principle 2.1 of the Recommendation attempts to fix the boundaries to this exception by limiting the collection of personal data to such as are necessary for the prevention of a real danger or the suppression of a specific criminal offence, unless domestic law clearly authorises wider police powers to gather information. 'Real danger' is to be understood as not being restricted to a specific offence or offender but includes any circumstances where there is reasonable suspicion that serious criminal offences have been or might be committed to the exclusion of unsupported speculative possibilities. By way of example, reasonable suspicion that unspecified drugs were being illegally brought into a country through a port by unidentified private yachts would justify the collection of data on all such yachts using that port, but not all yachts, their owners and passengers using every port in that country."
>
> (Explanatory Memorandum, para. 43)

The Recommendation is also strict as concerns the collecting of **sensitive (racial, political, religious or sexual) information on individuals**, or on their **membership (or associations with) lawful groups or movements**. Principle 2.4 sets out very strict limitations on such police data gathering - which are of particular interest to this study in view of the trends in police activity identified in our earlier papers:

> "The collection of data on individuals solely on the basis that they have a particular racial origin, particular religious convictions, sexual behaviour or political opinions or belong to particular movements or organisations which are not proscribed by law should be prohibited. The collection of data concerning these factors may only be carried out if absolutely necessary for the purposes of a particular inquiry.

As the Explanatory Memorandum explains:

> "*Principle 2.4* treats the issue of sensitive data and reflects the concern expressed in Article 6 of the Data Protection Convention that the collection and storage of particular categories of data should be restricted. It may be the case that the collection of certain sensitive data will be necessary for the purposes set out in Principle 2.1. However, in no circumstances should such data be collected *simply* in order to allow the police to compile a file on certain minority groups whose behaviour or conduct is within the law. The collection of such data should only be authorised if 'absolutely necessary for the purposes of a particular inquiry'. The expression 'a particular inquiry' should be seen as a general limitation; such an inquiry should be based on strong grounds for believing that serious criminal offences have been or may be committed. The collection of sensitive data in such circumstances should, moreover, be 'absolutely necessary' for the needs of such inquiries.
>
> The reference to sexual behaviour does not apply where an offence has been committed."

The reference in this passage to "the purposes set out in Principles 2.1" underlines that sensitive data and group data of the kinds mentioned may, if at all (i.e. if "absolutely necessary"), be collected only in relation to a "*particular* inquiry", in which there are "*strong* grounds" for believing that "*serious* criminal offences" have been committed, or where there is a "*real danger*" that such offences will be committed. It would clearly contravene the Recommendation if such information were collected for general "preventive" or police "intelligence" purposes, even if those were to relate to "serious criminal offences", in the absence of such specific grounds for police action.

The Recommendation also clearly reflects the "constitutional" approach we noted in the selected countries, in its principles on **collecting data unbeknown to the data subject, and/or by special technological means** (Principles 2.2 and 2.3):

> "2.2. Where data concerning an individual have been collected and stored without his knowledge, and unless the data are deleted, he should be informed, where practicable, that information is held about him as soon as the object of the police activities is no longer likely to be prejudiced.
>
> 2.3. The collection of data by technical surveillance or other automated means should be provided for in specific provisions."

The Explanatory Memorandum adds:

> "*Principle 2.2* addresses the issue of the collection and storage of data without the data subject being aware of this and attempts to offer a regulatory principle when it is decided to retain the data so collected, namely the person on whom data have been collected without his knowledge should be informed that data are being held on him as soon as the object of the police activities is no longer likely to be prejudiced. Of course this procedure will be unnecessary if the police have decided to delete the data collected unbeknown to the individual.
>
> It is accepted that Principle 2.2 may prove difficult to implement where street videos and similar mass surveillance methods are an issue and information has been collected on a great number of persons. It is for this reason that the principle recommends informing those subjected to a secret surveillance that data are still held on them only 'where practicable'. The police themselves will be expected to take the decision.

> It is thought that member states may find this principle of value when considering the case-law of the European Commission of Human Rights which, in the context of Article 8 of the European Convention on Human Rights, has recognised that the collection and storage of data on an individual without his knowledge could raise an issue of data protection (Application No. 8170/78, X v. Austria, Application No. 9248/81, Leander v. Sweden).
>
> While Principle 2.2 places the emphasis on the storage of personal data collected unbeknown to the data subject, whether by secret means or non-secret means (for example, asking questions of the data subject's neighbours), *Principle 2.3* focuses on the collection of data by technical surveillance or other automated means. Specific provisions in national law should govern collection of data by such methods. In particular, the case-law of the European Court of Human Rights should be borne in mind when recourse is had to wiretapping. The judgment in the Malone case states that such a form of technical surveillance must be authorised with reasonable precision in accessible legal rules that sufficiently indicate the scope and manner of exercise of the discretion conferred on the authorities and be accompanied by adequate guarantees against abuse."
>
> (paras. 44 – 46)

The Explanatory Memorandum goes on to stress more generally the need, not just for the police to comply with **domestic law**, but also for such domestic law to conform to **the requirements of "law" as elaborated in the case-law of the European Court of Human Rights** (as discussed above, in section 2.2):

> "Law-enforcement agencies work within the confines of the law and their data collection activities are thus circumscribed. Accordingly, domestic legal provisions, which must take as their minimum basis the provisions of the Convention for the Protection of Human Rights and Fundamental Freedoms (1950), must be respected. In this regard, account must also be taken of the case-law of the European Commission and European Court of Human Rights in the areas of arrest or detention for questioning, search and seizure, methods of interrogation, the taking of body samples, fingerprints and photographs, etc. It goes without saying that the relevant domestic legislation must conform to the provisions of the Convention as interpreted by the European Court of Human Rights."
>
> (para. 47)

Principle 3 concerns *storage* of personal data for police purposes. It stipulates:

> "3.1. As far as possible, the storage of personal data for police purposes should be limited to accurate data and to such data as are necessary to allow police bodies to perform their lawful tasks within the framework of national law and their obligations arising from international law.
>
> 3.2. As far as possible, the different categories of data stored should be distinguished in accordance with their degree of accuracy or reliability and, in particular, data based on facts should be distinguished from data based on opinions or personal assessments.
>
> 3.3. Where data which have been collected for administrative purposes are to be stored permanently, they should be stored in a separate file. In any case, measures should be taken so that administrative data are not subject to rules applicable to police data."

Of particular interest to this study is the emphasis on classifying data in accordance with their degree of accuracy or reliability, and on **the need to distinguish facts and opinions or assessments**. A similar emphasis is placed on this in the principle setting out the "*conditions for communication*" of data, principle 5.5.ii:

> "As far as possible, the quality of data should be verified at the latest at the time of their communication. As far as possible, in all communications of data, judicial decisions, as well as decisions not to prosecute, should be indicated and data based on opinions or personal assessments checked at source before being communicated and their degree of accuracy or reliability indicated.
>
> If it is discovered that the data are no longer accurate and up to date, they should not be communicated. If data which are no longer accurate or up to date have been communicated, the communicating body should inform as far as possible all the recipients of the data of their nonconformity."

The reference in principle 3.1 to "storage of personal data for police purposes" should not be read as allowing data, collected and initially stored for one police purpose (e.g., in connection with the investigation of a particular offence) to be entered into all-purpose police databases, accessible by various police bodies for various police purposes. Rather, the Recommendation stipulates in principle 5.1 that:

> "The communication of data between police bodies to be used for police purposes should only be permissible if there exists a legitimate interest for such communication within the framework of the legal powers of these bodies."

This can be seen as expressing the same principle we noted in the national laws discussed above: that data collected for one police purpose may be used for another police purpose only if it could have been independently collected for that other purpose.

As concerns the *communication* of police data to non-police bodies, the rules in the Recommendation are rather complex and convoluted, but still reflect the "constitutional" principles of "necessity" and "proportionality".

Thus, personal data held by the police may be communicated to other (non-police) public bodies if:

- they are "**indispensable** to the recipient to enable him to fulfill his own lawful task"; and
- "provided that the aim of the collection or processing to be carried out by the recipient is **not incompatible with the original processing** [of the data by the police]"; and
- provided there are no "legal obligations of the communicating body" (i.e. the police body which is sending the data) which stand in the way of the communication

(principle 5.2.i.b)

They may also, "**exceptionally**", be communicated, "**in a specific case**", to public or private bodies, if:

a. the communication is undoubtedly in the interest of the data subject and either the data subject has consented or circumstances are such as to allow a clear presumption of such consent, or if

b. the communication is necessary so as to prevent a serious and imminent danger.

(principle 5.2.ii.a & b [public bodies]; principle 5.3.ii.a & b [private bodies)

The Recommendation also allows the communication of personal data held to the police to both public and private bodies, if:

> "there exists a clear legal obligation or authorisation, or with the authorisation of the supervisory authority."
>
> (principle 5.2.i.a [public bodies]; principle 5.3.i [private bodies])

The Recommendation adds, with regard to communication of data to private bodies only, that such an obligation or authorisation must exist "**in a particular case**" (principle 5.3.i).

In fact, as will be clear from the references, this is the first basis for such communications listed in the Recommendation, in both principle 5.2 and 5.3. The text might suggest that the legislator, or the bodies authorised to grant such authorisations, are given complete discretion in the matter - but that is of course not true. First of all, as the Explanatory Memorandum expressly stresses, *all* communications of this nature are "exceptional" (para. 58). Furthermore (although this could have been spelled out in more detail), the legal provisions permitting communication, or the *ad hoc* authorisations for communication, must of course still comply with the "constitutional" requirements of *inter alia* the European Convention on Human Rights. They must be "necessary" and "proportionate" and set out in clear, precise language, in published rules; and they must be subject to appropriate safeguards and control. As it is, this is only hinted in the Explanatory Memorandum where it says that:

> "The 'clear legal authorisation' referred to in Principle 5.2.i.*a* could be provided by a magistrate."
>
> (para. 60)

The Recommendation is similarly not very developed as far as **interconnection of files** and **on-line access to data from other (non-police) public and private bodies** is concerned. This is undoubtedly because of the Recommendation's age: it was drafted at a time, almost 20 years ago, when data matching was hardly conceived. Principle 5.6 states

> "The interconnection of files with files held for different purposes is subject to either of the following conditions:
>
> a) the grant of an authorisation by the supervisory body for the purposes of an inquiry into a particular offence, or
>
> b) in compliance with a clear legal provision.
>
> Direct access/on-line access to a file should only be allowed if it is in accordance with domestic legislation which should take account of Principles 3 to 6 of this Recommendation."

The comments above, concerning "clear legal provisions" and "authorisations" again apply: these should conform to the "constitutional"/European principles. This time, the Explanatory Memorandum goes some way towards spelling that out:

> "While Principle 2 constitutes a general principle for the collection of data by the police, *Principle 5.6* concerns the particular situation where the police may seek to collect data by linking up its files with files held for different purposes, for example social security bodies, passenger lists kept by airlines, trade union membership files, etc. Alternatively, it may be sought to match up a number of files to see if they provide a clear profile of a certain type of delinquency and the sort of persons likely to engage in such delinquency.
>
> The legitimacy of such practices is made conditional on the grant of either of the types of authorisation laid down in *a* and *b*. **The 'clear legal provision' referred to in Principle 5.6.*b* should state the conditions under which interlinkage can take place.**
>
> The possibility of the police having a direct computerised access to files held by different police bodies or by other bodies is discussed in the final sub-paragraph of Principle 5.6. **Direct access in these circumstances must be in accordance with domestic legislation which should reflect certain key principles of the Recommendation**."
>
> (paras. 78 – 80, emphasis added)

By contrast, the Recommendation is quite strong on **data subject rights**, setting out clearly the strict conditions under which access etc. can be denied, and providing extensive safeguards in the form of motivated decisions, supervision by the data protection authorities, keeping access requests separate from the main police files, etc. (see principle 6 and paras. 81 – 95 of the Explanatory Memorandum).

The Recommendation also stresses (indeed, in the very first principle) that:

> "Each member state should have an **independent supervisory authority outside the police sector** which should be responsible for ensuring respect for the principles contained in this Recommendation."
>
> (principle 1.1, emphasis added; see paras. 31 – 33 of the Explanatory Memorandum).

4. Conclusions

This paper has shown that there is a highly-developed, "constitutional" approach to fundamental rights, derived from the constitutional traditions of the Continental-European States and developed by the European Court of Human Rights under the European Convention on Human Rights. This approach has also been adopted by the European Court of Justice.

We have further shown that, in spite of the unusual nature of data protection, this approach is also adopted by the European Courts with regard to data protection issues, both in general and with regard to the processing of personal data in the police sector. The Council of Europe has furthermore developed a set of principles on the latter issue, which has come to be taken as the standard in this field.

We have also noted that, under both European and UK law, the United Kingdom authorities are now obliged to adhere to these principles. The UK courts, and more importantly for the present study, the UK Information Commissioner, are legally bound to also adopt this approach in their assessment of cases and issues in this area.

In our final paper, we will further discuss the detailed implications which this has for the work of the Information Commissioner, especially in view of the technical and political developments in the law enforcement area, which we identified in our earlier papers. There, we will both argue that the adoption of this "constitutional"/European-legal approach to data protection is not only legally compulsory, but also essential if the UK is to meet the major challenges in terms of fundamental rights, data protection, and law enforcement which we believe are on the horizon (or even already with us). We will, in that final paper, both indicate the specific implications of the "constitutional"/European approach in specific, selected areas, but will also seek to provide the Commissioner with practical "check-lists" in these matters. And we will make specific proposals on how the Commissioner could - and in our view should - seek to further compliance with the basic principles adduced in this paper.

- o – O – o -

DK, Cambridge/London, February 2004

fipr

Foundation for Information Policy Research

UK INFORMATION COMMISSIONER STUDY PROJECT:

PRIVACY & LAW ENFORCEMENT

Paper No. 5:

conclusions & policy implications

February 2004

5. Conclusions & Policy Implications

Acknowledgements: The authors would like to acknowledge the following people and organisations for their cooperation and advice: Advisory Panel members Richard Clayton, Eileen O'Keefe, Peter Sommer, Simon Watkin and Paul Whitehouse and members of the Advisory Council of FIPR. Phillip Webb, Kevin Robson and Fred Preston of the Police Information Technology Organisation. Gus Hosein of the LSE and Simon Davies of Privacy International.

1. Introduction

This paper builds on our previous four papers. It recalls the challenges which the Information Commissioner will face in the near future (if not already), both in general and with regard to law enforcement and wider State control (below, 2). It then identifies the general implication of these challenges for the Commissioner's overall role and approach, in legal and policy terms (below, 3), before discussing certain specific matters to be addressed in terms of data protection, privacy and law enforcement (below, 4).

2. The challenges facing the Information Commissioner (a recap)

We have shown in our first two (combined) papers that as a result of technical (especially information technology-) developments, in the next five years we can expect an explosive increase in the generation, retention and availability of personal data. Everything we do - our movements, communications, transactions - will leave detailed data trails which can be captured, analysed and used by those with access to them in their interactions with us and their decisions about us. And we have also shown that there is a further trend towards a reduction in the functional separation between public entities, and a change in the boundaries between the public and the private sectors.

Specifically, partly as a result of a drive for "joined-up Government" and increased efficiency, the "bell curve" of criminality and other forms of social control is being expanded and flattened: activities which did not use to be criminalised are increasingly brought within criminal law; and there is an increased blurring between criminal and other (after the fact) sanctions and other (preventive) measures of State control. "Good parenting" is imposed by order, "bad parenting" is penalised; parents are fined for truancy by their children; the Government wants to bring in random searches for drugs of pupils in schools. The State is increasingly looking for a wider range of measures which it can adopt against certain targeted groups: religious "sects" suspected of (often rather ill-defined) exploitation or abuse of their members, suspected football hooligans, suspected paedophiles or rapists, or suspected supporters of (not-necessarily unlawful) "extremist" movements; etc.

Many of these measures apply even though the targeted individuals have not been convicted of any specific criminal offence; indeed, often, no offence needs to have been committed. Most crucially depend on information-gathering, increasingly combined with sophisticated data analysis and on predictions based on such analyses. All involve, or may involve, the police and other law enforcement and non-law-enforcement agencies working together. All this will lead to ever-greater data exchanges between public bodies and between public and private bodies.

Police work will thus become increasingly part of wider social (State) policies. As we put it in that first combined paper (on the basis of an interview with the Chief Executive of the Police Information Technology Organisation):

5. Conclusions & Policy Implications

> "the police informational environment will in the future become fused with a vast spectrum of non-police organisations and data reserves: moving progressively from regional *unit*, to police *family*, to law enforcement *community* and finally to a full societal *alliance*."

As we noted in our fourth paper (with reference to an earlier study for the European Commission), this change in the police informational environment - this increased blurring of the boundaries between police work and other areas of State policies - is linked to **a change in the objects and nature of police work itself**. From at least the 1970s onward, the presumed general increase in criminality, but more in particular the new threats to society posed by drugs-related and other organised crime, and especially by terrorism, led to a very significant extension of the role of the police from their traditional tasks:

- **the investigation and prosecution of specific criminal offences**; and
- **the countering of (real and immediate) threats to public order**.

into a further, previously much more marginal area:

- **prevention** of criminal offences being committed, or of threats to public order materialising - or indeed (in line with the trend noted above), of other activities which are deemed to be socially damaging or unacceptable, even if they are not necessarily criminal.

This relatively new are of police work is typically **intelligence-led**. In practice, it involves:

- the collecting of personal data on a **wider range of data subject**: i.e. not just on persons (reasonably) suspected of involvement in a criminal offence, or who pose a clear and immediate threat to public order (the targets of "classic" policing), but also on persons who "*might*" be involved in, or who "*might become*" involved in, (certain, not always very-well-defined types of) "serious" crime or disturbances and indeed on people who are "*in contact with*" such already ill-defined targets;

- the increased use of **more intrusive, secret means of data collection** (telephone tapping, "bugging" of homes and offices, the use of informers and undercover agents, etc.) against this wider range of objects of police enquiries;

- **more intrusive means of data processing** including, in particular, ever-wider **"data matching"** and "**profiling**" including the screening of various (not necessarily only police- or public sector-) databases to "filter out" from a *general population*, individuals who are deemed to merit further police attention of the above kind;

- **an increased blurring of the distinction between the work of the police and the work of the intelligence services**, on the one hand, **and the work of social and other State services** (such as the NHS, immigration), on the other (the new "full societal alliance" mentioned above);

- **increased centralisation** within countries (including the UK); and

- **increased internationalisation**, especially within the EU but also (more problematically in terms of data protection) with the USA and other Western countries (especially those which are members of, or have special arrangements with, NATO).

5. Conclusions & Policy Implications

In our third paper, we discussed the "**Total Information Awareness**" system in the USA and the related controversy over the transfer of **airline passenger (so-called PNR-) data** from the EU to the USA. We believe that even though the TIA-program has, for now, been suspended, it still represents the ultimate step in moves towards preventive, intelligence-led law enforcement. In a way, it is the natural outcome of the above trends. If the programs being developed under the TIA banner - "next-generation face recognition", computerised translation of texts in foreign languages, computer-assisted data analysis, etc. - were to be shown to be effective in the fight against terrorism, there would be an unstoppable demand for their introduction in the fight against serious or organised or international crime (which is in any case inseparable from the fight against terrorism).

A particularly problematic aspect of this technology-driven, "intelligence"-based policing-as-part-of-wider-social control (as again well illustrated by TIA), is **the trend to classify people on the basis of supposedly highly-sophisticated pattern-recognition and -re-defining programs**. If computers can reliably classify a person as a "potential terrorist", they can surely also single out people who are likely to have committed a bank robbery or a rape, or some other heinous crime? Indeed, it would be useful if the system could predict who *will* rob banks, or *will* rape people...

We believe we have shown that TIA-type programs of this kind have a long way to go to live up to this promise and that their usefulness even in the fight against terrorism is doubtful. However, we believe that the above trends - unless countered - will nevertheless result in **a wider use of such computer "profiling", of larger sections of the population, for a range of purposes**, irrespective of such doubts.

There are clear and inherent dangers in the establishment of any secret Government databases or file collections, even of the old-fashioned, primitive kind, as the ECHR-cases of Leander and Rotaru, discussed in our fourth paper, have shown. If such processing is extended and based on supposedly more sophisticated, but at the same time less-controllable computer technology with built-in (but unacknowledged) biases, this will have **a more than just chilling effect on democratic freedoms**. They could lead to the stigmatisation of minorities and ethnic, religious or cultural "out-groups" and can be used to harass political activists and others - with the basis for such stigmatisation and harassment hidden in impenetrable algorithms. Leander was denied a job on the basis of an "error-ridden" secret file; Rotaru was falsely classified as a right-wing extremist in 1949 and half a century later still nearly denied compensation for the persecution he suffered in Communist Romania because of this file. Bigger and more powerful databases are no less susceptible to such errors. In the USA, political activists have already been "flagged" and prevented from travelling, without any serious evidence that they were involved in crime (let alone terrorism). In Britain, 30,000 Muslim homes have been raided under anti-terrorist legislation, presumably on the basis of "intelligence", with less than 0.5% of such raids resulting in terrorism-related arrests.

Although there will also be technological advances in "**privacy-enhancing technologies**" (PETs), these will not be able to match the loss of control that individuals will suffer with regard to the collection, storage, exchange, analysis and use of their data. The principle of consent as the basis for personal data processing ("informational self-determination") is already largely illusory. It has lost all meaning with regard to the processing of personal data in the law enforcement sector (in the wide sense used above), where secrecy rather than transparency is the rule.

In sum: ***Policing in the early-21st century increasingly extends beyond the traditional police tasks of investigation and prosecution of crime and the countering of immediate threats, to "preventive" action against suspected criminals, and indeed against not-necessarily-unlawful actions which are nevertheless deemed to be socially unacceptable or indicative of possible future illegality. At the same time, policing (for all these ends) has become more sophisticated, more intrusive, more centralised, and more secret, than ever since the Second World War. And the trend is towards yet greater merging of police work with other State activties aimed at ensuring comprehensive social control, yet more sophistication, yet more intrusion, yet more central governmental (and intergovernmental) control, and yet greater secrecy.***

3. General implications for the Information Commissioner: the need to adopt a "constitutional" approach to privacy, data protection and law enforcement

The above-mentioned developments have a serious impact on human rights and civil liberties, and more generally on the relationship between the individual and the State. The idea that State authorities should have unrestricted access to all the data in extremely large (and by their very size sensitive) public- and private-sector databases, on millions of people, without any need to prove the relevance or necessity of access to data on any particular individuals, and that they should be allowed to carry out extensive "profiling" and "risk assessment" of such entire populations, is anathema to the most fundamental principles of data protection and the rule of law. Yet that is the trend.

Our analysis of these matters thus shows that ***the European data protection authorities - and in the UK, the Information Commissioner - have a much more important role to fulfil than previously realised. They are not just the guardians of some rather obscure and impenetrable pieces of legislation, to be used mainly against unwanted direct mail or errors in credit files, but must become the main defenders of individuals against the over-powerful, data-fed machinery of the State that could result from the trends identified above.***

In theory and in very broad terms, it is easy to claim that this is a simple matter of balancing different interests, of common-sense guidance. As the Working Party established under Art. 29 of the EC Framework Directive on data protection put it:

> "It is not proved that not taking into account properly the principles of proportionality and data minimization results into more efficiencies in combating terrorism and maintaining internal security, whilst respecting those principles constitutes an essential guarantee for safeguarding citizens' rights ... [T]he legitimate requirements of internal security and fight to terrorism can be pursued in a proportionate and reasonable way through systems which are in line with the fundamental principles of privacy and data protection."

It is also clear, however, that in such a stand for fundamental rights and against ubiquitous surveillance, the odds are heavily loaded against the Information Commissioner. As recent developments in the Soham murder trial and other instances have shown, the claim that data protection merely serves to protect the guilty and that law-abiding citizens have nothing to fear from uninhibited data sharing and mining is forceful, even if untrue.

Matters are complicated by a current lack of concern on the part of the general public. Most people do not perceive increased surveillance as a threat, indeed approve of extensive powers

of data retention and exchange, e.g., by means of CCTV. Data protection cannot be an activists' niche: the Commissioner will not be effective unless the public accepts that individual data needs to be protected. However, we believe that there is increasing recognition of the issues. In the private sector, there is increasing concern about the use of personal data by employers, financial institutions, insurance companies, etc. The same applies, e.g., to uncontrolled data sharing in the NHS. The proposed national children's' database is (we believe) likely to lead to public scandal. As far as law enforcement authorities are concerned: what if the state is able to identify all those participating in a demonstration? If the police had had, and had used, such technology, it would have been able to put more than 1 million people on a database in connection with the Stop the War in Iraq demonstrations in 2003. Would all those have been content with that? Or with further use of such information, e.g. if they subsequently applied for a government job?

We believe that the low level of current concern will end with increased awareness; that data collection/retention/disclosure/sharing/analysis/use will become a hot political issue in the near future, as more and more people are affected by such activities and become aware of their effects. And we submit that this is desirable: that the public should be made aware of the implications of the above-mentioned trends and encouraged to take an active stand on them.

We believe that the above has a number of implications for the work of the Information Commissioner in the field of law enforcement. First of all, it reinforces the importance of the Commissioner's "missionary" activities: of his efforts to inform the general public and data controllers of the requirements of the law, of his public stands and statements, and of his detailed reporting on the operation of the law. It will also be crucial for the Commissioner to convince law enforcement and other agencies of the need for restraint and strict control, if they want to continue to police by consent rather than (information) power.

However, secondly, and from the point of view of this study most importantly, we believe that the above-mentioned trends, and the threats they pose to democracy and the rule of law - as well as certain legal considerations - demand that **the Information Commissioner should define his role, at least in respect of data processing for law enforcement purposes, in unambiguously "constitutional" terms.**

In the United Kingdom (or at least in England and Wales), there is a traditional reluctance to adopt such a stand - especially *vis-à-vis* the legislator. In particular, the courts, and regulators such as the Information Commissioner and his predecessor, the Data Protection Registrar, have tended to defer to Parliament on the basis of the doctrine of "sovereignty of Parliament". This has meant that the courts, and even more such regulators, have been unwilling to challenge derogation clauses in formal statutes which limited or set aside provisions in the statutes they were asked to interpret, apply or implement. "Statutory overrides" (as we shall call them) generally were - and still are - accepted as placing the matter in question outside of the scope of the judicial or regulatory supervisory body in question. They typically apply in the area of law enforcement and data sharing.

In our fourth paper, we have shown that from a European perspective, such matters should <u>not</u> be left unassessed: on the contrary, ***the "quality" (clarity, precision and foreseeability) of the basic statutory rules and of any "statutory overrides" or exceptions must be checked by reference to European standards, derived from the European Convention on Human Rights and "general [constitutional] principles of European Community [and –Union]***

law". What is more, as explained in Paper No. 4, as a result of the Human Rights Act and the European Community Acts, ***the UK courts and the UK Information Commissioner, too, must check such legislation, and such exceptions, by reference to these European/ "constitutional" principles***.

We believe that this is the single most important, general recommendation we can make. In our opinion, as explained earlier, it will only be through the adoption of such an approach that the Information Commissioner will be able to counter the democracy-threatening trends we have identified. Furthermore, it is manifest from the case-law of the European Court of Human Rights and the European Court of Justice, described in Paper No. 4, that these standards must already be applied by the UK authorities. These standards are "directly applicable" under the HRA and the ECA. The Commissioner is not just entitled, but under European and UK law already required, to apply these tests.

We submit that it is therefore essential to see the Information Commissioner as a guardian of a fundamental, constitutional right rather than as a bureaucratic regulator of a technical law - and that it is imperative that the Information Commissioner too comes to see himself in this light. In assessing UK laws and regulations, and practices under these laws and regulations, the Information Commissioner should focus on the constitutional (ECHR/HRA/EU) implications of data collection/retention/sharing/use, rather than on the narrow, legalistic terms of the DPA; and he should take a harder enforcement view (rather than his current highly conciliatory approach), especially with regard to data protection and law enforcement. We do not believe this requires a change in the law, only a change in attitude on the part of the Information Commissioner.

This has particular relevance with regard to both the drafting and adoption, and the operation in practice, of "statutory overrides" (statutory exceptions/exemptions/derogations from the normally-applicable data protection rules and –principles and the rules built on such exceptions etc.), as typically provided for with regard to law enforcement and state control (in the new, wide sense noted above): this is where there is the greatest temptation for the government to introduce exceptions/exemptions/derogations; this is where they have the greatest impact on individual rights. The traditional UK approach, based on the concept of sovereignty of Parliament and (thus) of narrow interpretations, is often no longer sufficient (as the ruling of the Court of Appeal in Durant has shown).

Secondly, ***we suggest that to be effective, this approach must tie in with new UK arrangements under the HRA, through which the substantive provisions of the ECHR have become directly applicable in UK law*** (although the ECHR requirements in some respects extend beyond HRA requirements, in particular as concerns processing of personal data by private-sector bodies, and as concerns the "right to a remedy": see Paper No. 4).

Thirdly, we propose that, in view of the internationalisation of policing, ***the approach must also seek to tie in with views of data protection authorities in other EU Member States***, as expressed in particular in the opinions and working documents of the Working Party established under the EC Framework Directive on data protection (*idem*).

5. Conclusions & Policy Implications

Before discussing the implications of such a European/"constitutional" approach (as we shall call it), we must stress that ***the above is not only a legal/constitutional/ECHR/HRA imperative, but also an operational one***: If the UK rules do not conform to European minimum standards, other EU forces could be constitutionally prevented from disclosing data to or sharing data with their UK counterparts. And even if the UK were to meet the minimum standards, but adopted significantly different approaches or rules on specific issues, the resulting divergences would still create obstacles to effective international policing and -police co-operation – and more in particular to the data pooling/transfer/exchanges that are increasingly part of this effort.

Specifically, as noted in our fourth paper, ***there are four closely related matters which should inform all advisory, supervisory, complaint support- and enforcement actions of the Information Commissioner in this area***:

(1) Since data collection/retention/disclosure/sharing/use constitutes an interference with the right to private life (Art. 8 ECHR), it must be based on "**law**" and be "**necessary** in a democratic society" to serve a "**legitimate aim**." These terms imply more specific tests:

✓ in order to qualify as "***law***" under the ECHR/HRA, the rules covering such actions must be clear, strict, precise, detailed, published, and binding;

✓ the rules must not only ensure that certain data collection/retention/disclosure/ sharing-operations or -uses are "***necessary***" in general terms, but *each specific collection/retention/disclosure/sharing/use* of personal data must be "necessary" *in each specific case.* - and there must be procedures for ensuring this and for allowing subsequent verification (see point (4));

✓ for specific kinds of data or data processing operations, the "legitimate aim" or ***purpose*** will usually have to be spelled out in detail: merely stipulating that the data or the processing is "for the purpose of protecting public order" or "for the purpose of preventing or prosecuting criminal offences" will often not be sufficient - especially not in justifying specific interferences in the private life of individuals in specific cases;

(2) There must be **transparency** about data processing operations, both in general terms (cf. point 4 re reporting) and as concerns the **informing of data subjects**: data subjects should be informed of all processing of their personal data by law enforcement (and related) agencies, unless there is a clear necessity not to do so, and in the latter case there must be ***alternative safeguards*** (see next two points);

(3) There must be "**effective remedies**", effectively available to data subjects, against (alleged) improper collecting/retention/sharing and use of their data; and

(4) There must be general, **independent supervision** over intrusive collection/disclosure/ retention/sharing/use of personal data by law enforcement agencies, and by others for law enforcement purposes. This must include independent **audits**, and full, informative **reporting** on the matters reviewed.

In wider terms, the Information Commissioner's role is therefore to ensure (insofar as this is within his powers) that all collection/retention/ disclosure/sharing/use of personal data for law enforcement/policing purposes in the UK meets these European/"constitutional" legal standards.

This requires the Information Commissioner to provide **serious input in primary legislation**, and **close reviews of subsidiary rules and regulations**. It also requires him to hear **complaints** from individuals, to act as the **independent supervisory body** concerned, to carry out (or assist in) **audits**, and to **report** in detail on the issues raised. Most crucially, the Information Commissioner should carry out these functions explicitly by reference to the European/"constitutional" principles we have discussed in Paper No. 4. In the next section, we will discuss these specific matters in more detail.

4. Specific matters to be addressed

Note: Within the Information Commissioner's office, there is already a specialised team dealing with the application of the Data Protection and Freedom of Information Acts to the law enforcement and justice sector, and overseeing compliance with the law by relevant data controllers. The team also takes the lead in developing the Commissioner's policy on the meaning of "good practice" in the sector. Many of the matters mentioned below would fall within the remit of this team, but others (such as the handling of individual complaints) may involve other teams or departments within the Office of the Information Commissioner. We have not generally tried to make suggestions about intra-office divisions of responsibilities, but rather addressed our recommendations to the Information Commissioner in general.

4.1 Input in the drafting of primary legislation

We submit that, in line with the approach in certain Continental-European countries, the broad basis for all personal data processing by the police and other law enforcement agencies, for law enforcement purposes,[322] must be set out in **primary legislation**. What is more, the Information Commissioner is the most appropriate expert authority in the UK for any assessment of whether the rules in such primary legislation meet the relevant European/"constitutional" requirements (as listed at 3).

As explained, this assessment relates, in particular, to standards contained in (or derived from) the ECHR. We believe that the Information Commissioner should therefore seek to be closely involved in the process under the HRA under which the Government must certify the compatibility of any human-rights-sensitive piece of legislation with the Convention and the Act. We do not believe that this requires any statutory amendment: the Commissioner is already usually consulted on these matters. ***What we propose is that the Information Commissioner's views are conveyed to the relevant Parliamentary Committees, as part of the ECHR-compatibility certification process.*** It should be extremely rare for a Bill to be put before Parliament which concerns processing of personal data by law enforcement agencies if the Commissioner is of the opinion that certain features or provisions of the Bill are incompatible with the relevant European data protection principles, as applied under the ECHR. By and large, such bills do not deal with the detail yet, but merely set out broad principles, and exceptions, to be clarified in subsidiary rules. The main issue here is to clarify in what areas such further regulation is needed from the

[322] This study does not deal with processing of data by law enforcement agencies for non-police/law enforcement purposes, such as the keeping of employment records of police officers.

point of view of the European/ "constitutional" principles, i.e. where the primary rules do not meet the "quality" requirements of precision and foreseeability.

Most often, the Information Commissioner will therefore merely want to point to areas covered by such primary legislation for which additional, more detailed subsidiary rules are needed. This would include, in particular, broadly-phrased "statutory overrides" (provisions in primary legislation which allow for exceptions/exemptions/derogations from the basic rules for the purpose of protecting public order or preventing of prosecuting crime): as explained in Paper No. 4, it is a general requirement of European law that in cases of such exemptions or derogations, additional, specific and suitable safeguards are provided. As noted below, that should lead to the further involvement of the Commissioner in the drafting of such rules.

This has not been done in the past. Indeed, it has proven extremely difficult even for the Home Office to determine exactly how many "statutory overrides" there are in current legislation - although it is clear that there are a great many, and that they are often set out in broad terms incompatible with the new, "constitutional" principles we have adduced. ***We therefore recommend that the Information Commissioner should carry out (alone or in cooperation with the Home Office) a review of all primary legislation, to see where the statutory rules - and more in particular any "statutory overrides" - are too broadly-phrased to be compatible with the ECHR/HRA, and thus require either amendment to the law or further regulation in (binding) subsidiary regulations providing the safeguards mentioned.***

4.2 Input in the drafting of/review of subsidiary rules

Many matters relating to law enforcement cannot be fully or adequately regulated in primary legislation. It is perfectly acceptable that much is left to lower-level rules and regulations, and even that these are drafted (at least initially) by relevant law enforcement bodies (such as ACPO or committees of ACPO). Indeed, only lower-level regulations can adequately deal with the specific, intricate issues raised by the new technologies discussed in our earlier papers: the taking of DNA samples, the use of CCTV (and the obtaining of data from private-sector CCTV operators), access to private-sector data generally, access to communications data, the use of ID cards and the circumstances in which they must be produced, the use of computer-generated algorithms in the taking of highly sensitive law-enforcement-related decisions, etc.

However, such rules must meet the standards briefly summarised above, at 3, and discussed in more detail in Paper No. 4. In particular, they must be **clear, strict, precise, detailed, published, and binding**. Vague, internal guidelines do not suffice: the rules must be very clear about when exactly each of the above technologies can be used and for what specific purpose, with specific examples. The rules should contain **specific safeguards**, e.g. as to who can authorise certain measures, and how this is recorded. They must be binding, in that a breach must (at least) be a serious disciplinary offence; if the matters significantly affect individual rights they should be subject to a formal procedure for adoption, e.g. requiring the approval of the Home Secretary or indeed, in appropriate cases, the silent or express

approval of Parliament.[323] All these rules should be made public: individuals should know when they may be subjected to such technologies.

The rules should furthermore ensure that, in principle, individuals who have been subjected to intrusive data collection or use without their knowledge are **informed** afterwards. Exceptions should be limited to what is strictly necessary to protect ongoing operations or sensitive operational matters. Examples should again be given.

In addition, the rules should specify that **detailed records and meaningful statistics** are kept: on when intrusive measures are authorised, by whom, at whose request, against whom, how often, and for how long; on whether the individuals concerned were subsequently informed of the measures, or not - with detailed reasons given for any non-informing; etc. Such statistics should be publicly available, preferably on-line.

In an Attachment to this paper, we have set out a tentative "**check-list**" against which draft rules or regulations can be tested; the list is drawn up on the basis of the matters mentioned by the European Courts and in the relevant European recommendations, opinions and working documents, discussed in Paper No. 4.

We propose that the Information Commissioner be closely involved in the drafting of any subsidiary rules or regulations relating to the processing of personal data (in the widest sense) in the area of law enforcement. If not a statutory duty, it should at least become a standing convention that the Information Commissioner is always consulted on the details of such rules, and gives his views on them, publicly. This should involve a clear assessment of such rules by references to the "check-list".[324]

It should be extremely rare for such rules to be adopted unless the Information Commissioner has held them to meet the standards set out in the "check-list". In such rare cases, the Commissioner should, if issues of principle are concerned, be prepared to use his enforcement powers - which would allow for the possibility of a review of the rules by the Data Protection Tribunal and the courts. If needs be, the Information Commissioner should suggest to the Tribunal or the courts that the matter is referred to the European Court of Justice for a preliminary ruling, or he should support individual applications in appropriate cases to the European Court of Human Rights (e.g., by means of a third-party intervention in such cases).[325] We realise that this implies a much more forceful approach by the Information Commissioner than has been adopted to date, but believe that the challenges

---

[323] Note that this excludes the possibilities of certain matters affecting fundamental rights (such as intrusive personal data gathering) being regulated in non-binding codes of conduct (such as the proposed "voluntary code" which has been mooted in connection with communications data retention): in terms of the ECHR (and thus the HRA), a non-binding code cannot be "law" and therefore cannot provide a sufficient basis for the processing involved. More generally, the use of terms such as "good practice" and "guidance" in this respect often suggests that no binding rules are needed. We feel that the Commissioner should re-affirm the need for binding rules which meet the European/"constitutional" standards of clarity, precision and foreseeability.

[324] If a bill is put forward which envisages such subsidiary rules, it would be commendable if it specified that, for matters to be further regulated in subsidiary rules, the opinion of the Information Commissioner should be sought, and if it went on to stipulate that rules which did not obtain a positive opinion would require an affirmative Parliamentary procedure. That is similar to the situation in France. That however is a matter for Parliament, not the Information Commissioner.

[325] Cf. the third-party intervention by the Northern Ireland Human Rights Commissioner in a number of joint cases relating to the use of lethal force in the Province, in proceedings before the European Court of Human Rights in Kelly *et al.* v the UK, judgment of 4 May 2001

facing society, described in our earlier papers and summarised above, demand such a more assertive role.[326]

We further recommend that the Information Commissioner be closely involved to ensure that the statistics are meaningful and easily-accessible: see below, reporting.

4.3 Handling of individual complaints

As explained in Paper No. 4, it is a crucial European/"constitutional"-legal requirement that any rules allowing for intrusive data collection and –use also provide systems of **support and help to individual data subjects** who are faced with a problem involving the processing of their personal data. An easily accessible, impartial and independent body to hear complaints from data subjects and assess whether there have been breaches of the rules must therefore be in place. Under the DPA98, this task of course already falls on the Information Commissioner - also in respect of processing in relation to law enforcement.[327]

It will by now be clear that we feel that the Information Commissioner should position himself as a strong advocate for data subjects, as the main guardian of individual rights in the face of the technological threat described in our papers. We feel that current practice does not live up to this.[328] The Commissioner does not provide a detailed breakdown of the 12,000 (!) or so complaints he receives each year (other than to make clear that some 35% are related to consumer credit or the Telecommunications (Data Protection and Privacy) Regulations 1999). It is therefore unclear how many complaints or requests for assistance relate to law enforcement. However, the general numbers give a broad indication of the Commissioner's approach. In the majority of cases (58.2%) "advice" was given, apparently without a further detailed assessment of compliance or non-compliance.[329] In 28.2% (about 3,500 cases), such an assessment was made. Of these, 58% were held to have probably involved a breach of the law (16.3% of all cases, against 11.9% in which it was held that there was probably no non-compliance). That is about 2,000 cases of likely non-compliance in a year, exposed on the basis of complaints alone.[330] In 44% of these cases (i.e. in some 880 cases) this was apparently "verified." Yet there is no detailed information on how these matters were followed up.[331] In particular, it is unclear whether the Commissioner's office

---

326 As discussed in Paper No. 4, we feel that the recent judgment of the Court of Appeal in the case of Durant v the FSA failed to conform to the applicable European standards. In our view, rather than simply deferring to this judgment, the Information Commissioner should have suggested that the question of the interpretation of the concepts of "personal data", "processing" and "relevant filing system" be referred to the ECJ.

327 We believe that complaints relating to law enforcement matters are dealt with by compliance teams, rather than by the special team dealing with law enforcement and justice matters. However, we assume that the compliance teams closely liaise with the special law enforcement and justice team in such cases.

328 The figures given in the text below are from the Information Commissioner's latest (2003) Annual Report.

329 The figure was even higher in previous years: 60.7% in 2002 and probably 77.4% in 2001 (the latter number is deduced from the totals: the report says 27.4%, but this appears to be a typing error, since the figures only add up to 100% if this is revised to 77.4%).

330 Note that in 7.1% of all the 12,000 complaints - that is, in some 850 cases - assistance was "declined" even though the complainant met the "threshold criteria," i.e. although the request was made by a person who is, or believed him- or herself to be, directly affected by the processing in question; the person was properly identified as the data subject; the processing was identified; and the processing did concern personal data. No reasons are given for this refusal to assist so many complainants.

331 There is some information on criminal prosecutions, but this is somewhat confusing. The report says that "91 cases were put before the criminal courts and 80 of them resulted in conviction" - but the list of prosecutions that follows this statement contains only 11 names of defendants. It is possible that the word "case" refers to each charge: most of the defendants are charged with a list of (usually identical or similar) offences. This includes a small number of prosecutions of police officers for the sale of police information. In 2003, only 2 cases concerned non-notification - a reflection of a

seeks to ensure that non-compliance matters are addressed in a wider way than just in relation to individual cases. As far as we can see, there has never been an enforcement notice (or even a preliminary enforcement notice) issued to any law enforcement agency (or indeed to any public-sector controller). There is also no information as to how fully complainants are informed of the outcome of their complaint: of whether the processing was assessed for compliance with the law, or the outcome of such assessment, or of the follow-up in wider terms (i.e. of whether the Commissioner felt that, apart from redress in the individual case, the controller should have changed practice more generally, and of whether this view was followed). There has not been a survey of the "customer-satisfaction" felt by complainants with regard to the handling of their cases by the Office of the Information Commissioner. Anecdotal evidence suggests that complainants do not receive very detailed feed-back of this kind. This is particularly worrying as concerns law enforcement matters, in respect of which individuals are often kept in the dark.

We recommend that, at least as far as processing by law enforcement agencies is concerned, the Commissioner should seek to ensure that individual complainants are as fully informed of all the details relating to their case, and of all processing of their data, as is compatible with the DPA98 and with the requirements of effective policing (strictly interpreted). The Commissioner should take a strong stand on behalf of complainants over this matter, and over processing in this field generally, and keep them fully informed of the outcome of their cases and of any more systemic follow-up. The Information Commissioner should furthermore separately report on all the law-enforcement-related cases thus examined, giving both detailed case information (without disclosing personal information or endangering operational matters) and aggregate data, in statistical form (with examples): see below, reporting.

Of course, the complaints procedure is without prejudice to the rights of individuals to obtain redress, and **compensation**, through the courts. In appropriate cases, the Information Commissioner can **intervene** in such cases to clarify the law. ***We recommend that such interventions should be explicitly on the basis of the broad European/"constitutional" principles set out at 3 and in the Attachment (rather than limited to narrow discussions of the terms of the DPA98).***

4.4 General supervision (other than in connection with individual complaints)

In addition to acting as advocate for individual complainants, the Information Commissioner of course also already acts as the independent supervisory authority in respect of processing by law enforcement agencies (unless the matter falls within the jurisdiction of another special body).

This should entail the carrying out of **audits** - also and in particular of personal data processing by law enforcement agencies and of disclosures by private-sector entities to such agencies and v.v. The Information Commissioner should report on these audits, as noted below, at 4.5.

---

policy decision not to focus on such cases (they are far too numerous). This does suggest that the cases concerned more serious offences, more directly affecting data subjects.

However, we feel that it would be useful if the Commissioner were again use the "**check-list**" in the Attachment, to assess the level of compliance with the law *and with the European/"constitutional" requirements*, by law enforcement agencies and others (as concerns data exchanges between the private sector, other public bodies, and law enforcement agencies).

We recommend that on the basis of the "check-list", the Information Commissioner gives "marks" for compliance in the specific area concerned to the law enforcement agencies concerned (and to other bodies as concerns data exchanges between them and such agencies). For simple public-information purposes, this could include a "traffic-light" system, with red indicating that there are serious deficiencies in compliance; orange that there are some issues to be addressed; and green that the agency concerned is operating fully in accordance with the letter and the spirit of the (detailed) rules.

4.5 Reporting

The Commissioner reports on this work through his website and in his Annual Report. However, like similar reports of the data protection authorities in other EU Member States, the annual reports merely tend to give a rather general picture, with some highlights. The information on the website is good, but in respect of supervision over law enforcement data processing matters could be better - and would have to be expanded if the Information Commissioner were to adopt the functions we have outlined above.

We recommend that, at least as far as processing of personal data for law enforcement purposes is concerned, the Information Commissioner make available to the general public:

- ***all his opinions on primary legislation (see above, at 4.1);***
- ***all his views on subsidiary rules (see above, at 4.2);***
- ***detailed information on all complaints, including much more detailed statistics, as concerns complaints relating to data processing by the different law enforcement agencies and disclosures of data by private entities to such agencies and v.v. (see above, at 4.3);***
- ***the text of all his interventions in court proceedings (see above, at 4.3); and***
- ***the results of all audits in detail; and***
- ***the "traffic-light marks" awarded to the different law enforcement agencies in respect of their processing of personal data under each separate set of detailed subsidiary rules.***

In addition, we recall our recommendation that the Information Commissioner should ensure that law enforcement agencies keep **detailed information and statistics** on how they apply primary legislation and (especially) the detailed subsidiary rules to be drafted, e.g. on authorisations for intrusive data collection, on decisions not to inform data subjects afterwards, etc. (see above, at 4.2). ***We recommend:***

- ***that the Commissioner verifies the accuracy and meaningfulness of such data;[332] and***
- ***makes this information available, in full, on his own website (or through "mirrors" of law enforcement agencies' websites).***

- o – O – o -

Attachment: Suggested check-list for the assessment of (subsidiary) rules relating to processing of personal data for law enforcement purposes and of processing under such rules.

DK/Cambridge, February 2004

[332] In the past, statistics of this kind have sometimes been misleading, e.g. by providing a number for authorisations issued in respect of certain measures, without clarifying that each authorisation could cover a multitude of measures, against a range of targeted individuals.

Attachment

Suggested check-list for the assessment of (subsidiary) rules relating to the processing of personal data for law enforcement purposes and of processing under such rules

Nota Bene: The check-list set out overleaf is based on the requirements under the ECHR (and thus the HRA) and which flow from the "general principles of EC [and EU-] law", and on the requirements for sectoral rules and for data transfer to third countries, developed by the Working Party of EU data protection authorities, established under Art. 29 of the EC Framework Directive on data protection (Directive 95/46/EC, which is the basis for the UK Data Protection Act 1998), as set out in more detail in Paper No. 4, the legal framework.

This check-list should be used for each distinct set of subsidiary rules applicable to distinct data processing operations for law enforcement purposes, such as, e.g.:

- ✓ **the rules on when DNA samples may be taken/when the data may be retained (and for how long)/when they may be disclosed, shared or accessed/and when and how they may be used;**
- ✓ **the rules on CCTV- and similar surveillance by private and public bodies, on the co-operation between such bodies, and on the data collection/retention/disclosure/ sharing/use of data (including sound and image data) captured in this way;[333]**
- ✓ **the more general rules on the making available of personal data by private entities (such as employers, retailers or financial institutions) to law enforcement agencies;**
- ✓ **the rules on the collection/retention/disclosure/sharing/use of communications data;[334]**
- ✓ **the rules on ID cards; and**
- ✓ **the rules on the use of computers in the taking of decisions which significantly affect individuals.**

It is an underlying assumption that detailed rules must be drawn up for each such distinct kind of operation: see the main body of this paper.

---

333 This area may need to be covered by several sets of rules, to deal with: the use of CCTV by private entities (including the rules on when, and subject to what procedures, private-sector controllers may or should hand over CCTV data (tapes) to law enforcement agencies; the use of CCTV by public entities (and more in particular by law enforcement agencies); and the circumstances in which law enforcement agencies may demand access to CCTV-data held by other (private or public) bodies, and related procedures.

334 Data and data processing relating to telephone-, fax-, email- and other communications may be subject to special oversight by a different UK Commissioner and may, to that extent, not be subject to oversight by the Information Commissioner. However, some of the data collection/retention/disclosure/sharing/use involved may be subject to the Information Commissioner's jurisdiction. Furthermore, to the extent that the check-list seeks to ensure compliance with "constitutional" standards (ECHR/HRA, EU Directives), the other Commissioners concerned would have to carry out similar checks.

CHECK-LIST

I. PRELIMINARY

1. ambit of the rules:

Does the matter regulated in the rules under consideration involve "*automated processing*" of "*personal data*", or "*processing*" of such data held in structured "*personal data files*", by law enforcement authorities, or the "*disclosure*" of such data to such authorities for law enforcement purposes?

Note 1: Contrary to the judgment of the CA in Durant, the above terms must be given a **wide** meaning: the Information Commissioner should apply the law (the DPA98) to **all information** in automated databases or structured manual files directly or indirectly related to identifiable individuals (e.g., not just by name or file number, but also by means of ID numbers, or index numbers, or indeed fingerprints or DNA or face-recognition systems). He should emphatically not limit his assessments to information affecting purely private matters, and he should especially not exclude information relating to "activities of a professional or business nature" or to information on political activities or alleged criminal acts, even if of a public nature or carried out in public.

Note 2: In terms of the ECHR/HRA, if the answer to the above question is affirmative, the processing must be regarded as *ipso facto* constituting an "interference" with the right to private life, which is only allowed if it is "in accordance with law" and "necessary in a democratic society" for a (specific) police purpose (as further clarified below).

2. preparation of the rules:

Has there been adequate consultation with interested civil society groups/NGOs in the preparation of the rules? Have comments or suggestions from such sources been taken into account?

Note: Consultation on primary or subsidiary rules is not a formal requirement. However, the importance of such consultation is stressed by the Working Party in other contexts and would lend legitimacy to any rules in this area.

3. European context:

Are there European guidelines in the area concerned (apart from Recommendation R(87)15 *regulating the use of personal data in the police sector*, e.g., in the form of Opinions or Working Documents of the EU Working Party on data protection)? Are the rules in line with that Recommendation and these other European standards?

Note: In answering the questions below, conformity or non-conformity with such European guidelines should be noted and (where necessary) explained. A significant departure from rules reflecting a clear "European consensus" - in particular, from the Recommendation - suggests that the rules are not "necessary in a democratic society".

II. DETAILED ASSESSMENT

4. is the processing regulated by "law"?

- is there a **legal basis** for the processing in ***primary legislation***?
- are there more **specific legal rules** relating to the **particular kind of processing operation** in question?
- are these specific legal rules **published**?
- are they **binding**?

5. does the processing serve a sufficiently-precisely "specified purpose"?

- What is (or was) the specific purpose for which the data are (or were) originally collected?
- If this is a law enforcement purpose, is the data collection/retention/use necessary for that purpose?
- If the data were not originally collected for a law enforcement purpose, is it necessary to override the purpose-limitation principle for a law enforcement purpose?
- How do the rules ensure that the data are only collected/retained/used if this is necessary in a specific case? What procedures are in place to ensure this (authorisation by senior officer; record; audit: cf. below, oversight)?

  Note 1: It is not sufficient to specify that processing serves "the police task", or even a specific police task (investigation and prosecution of crime; countering immediate threats; more controversially, "prevention"). It is important to be as precise as possible.

  Note 2: Personal data, collected for one specific police purpose (e.g. countering threats) can only be used for another specific purpose (e.g. investigating offences) if the data could have been independently collected for that second purpose.

  Note 3: Personal data should never be collected by the police or other law enforcement agencies "just in case".

6. is the processing "necessary in a democratic society" for the specified purpose?

A. do the rules cover all the "**core contents principles**", i.e.:

- ***the purpose limitation principle***: see above, at 5.
- ***the data quality and proportionality principle*** - data should be accurate and, where necessary, kept up to date. The data should be adequate, relevant and not excessive in relation to the purposes for which they are transferred or further processed. How is this ensured?
- ***the transparency principle*** - individuals should be provided with information as to the purpose of the processing and the identity of the data controller, and with other,

additional information insofar as this is necessary to ensure fairness. The only exemptions permitted should be in line with the Articles 11(2) and 13 of the Framework Directive. How is this ensured?

- ***the security principle*** **-** technical and organisational security measures should be taken by the data controller that are appropriate to the risks presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process data except on instructions from the controller. How is this ensured?

- ***the rights of access, rectification and opposition*** **-** the data subject should have a right to obtain a copy of all data relating to him/her that are processed, and a right to rectification of those data where they are shown to be inaccurate. In certain situations he/she should also be able to object to the processing of the data relating to him/her. The only exemptions to these rights should be in line with Article 13 of the Framework Directive. How is this ensured? If it is not ensured, note the alternative safeguards (cf. below, at

- ***restrictions on transfers to other bodies*** **-** transfers of the personal data to other bodies (in the UK, in the EU, but especially in third countries) should be permitted only where the recipient affords an adequate level of protection, either in general or in the specific sector concerned (i.e., here: in the law enforcement sector), by means of laws or other (binding) rules or special (international) agreements. Is this ensured?

B. do the rules provide for **additional principles** to be applied to specific types of processing such as:

- ***sensitive data*** **-** where 'sensitive' categories of data are involved (those listed in article 8 of the Framework Directive), additional safeguards should be in place, such as a requirement that the data subject gives his/her explicit consent for the processing. Recommendation R(87)15 stipulates that:

  "*The collection of data on individuals solely on the basis that they have a particular racial origin, particular religious convictions, sexual behaviour or political opinions or belong to particular movements or organisations which are not proscribed by law should be prohibited. The collection of data concerning these factors may only be carried out if absolutely necessary for the purposes of a particular inquiry.*"

  Is this principle set out in the rules? How is adherence to it ensured?

- ***automated individual decision*** **-** where the purpose of the transfer is the taking of an automated decision in the sense of Article 15 of the directive, the individual should have the right to know the logic involved in this decision, and other measures should be taken to safeguard the individual's legitimate interest.

  Note: The scope and application of this principle is still rather unclear. However, it could be invoked with regard to "profiling", if such techniques were to have actual repercussions for the individuals concerned (e.g., if they were to result in intrusive surveillance). It is clear that the use of such "profiling" techniques must be subject to a particularly strict "necessity" and "proportionality" test (and surrounded with particularly strong safeguards: see below)

C. do the rules lay down **appropriate limits** on the statutory powers "such as":

- a precise description of "the kind of information that may be recorded";

- a precise description of "the categories of people against whom surveillance measures such as gathering and keeping information may be taken";[335]

- a precise description of the circumstances in which such measures may be taken;

- a clearly set out procedure to be followed for the authorisation of such measures;

- limits on the storing of old information and on the time for which new information can be retained;

- explicit, detailed provision concerning:

  - ✓ the grounds on which files can be opened;

  - ✓ the procedure to be followed [for opening or accessing the files];

  - ✓ the persons authorised to consult the files;

  - ✓ the nature of the files;

  - ✓ the use that may be made of the information in the files;

  Note: the collection of data on "contacts and associates" (i.e. on persons not suspected of involvement in a specific crime or of posing a threat), the collection of information through intrusive, secret means ('phone tapping; "bugging"; informers; agents), and the use of "profiling" techniques, and indeed "preventive" policing generally, must be subject to a particularly strict "necessity" and "proportionality" test (and surrounded with particularly strong safeguards: see below).

D. do the rules ensure sufficient **transparency**:

- is the processing subject to notification?

- do the rules specify that data subjects have to be informed of the collection of data on them, whenever possible, and if not possible at the time, as soon as possible afterwards?

---

335 Note that the European Court of Human Rights in its Rotaru-judgment clearly regarded the gathering and keeping of information for intelligence files as, as such, "surveillance measures". This was not qualified by reference to the means used: "surveillance" is not limited to secret, technical means; it can also be kept on individuals by collecting information openly, or from public sources, e.g. from lists signed by people opposing the War In Iraq, or newspaper cuttings, or open photography or videoing of demonstrations.

- to what extent and how can data subjects exercise their data subject rights? are any restrictions on the exercise of these rights limited to what is strictly necessary to protect legitimate law enforcement activities? Are these restrictions lifted as soon as possible?

E. do the rules provide for adequate **procedural/enforcement mechanisms**, such as, in particular:

- **internal supervisory mechanisms** which effectively ensure a good level of general compliance. Is there a system of ***dissuasive and punitive sanctions***? Are these effectively enforced?

- **support and help to individual data subjects** who are faced with a problem involving the processing of their personal data? Does the Information Commissioner have jurisdiction in this regard, and full powers of access and review?

- **appropriate redress in cases of non-compliance**? Can a data subject obtain a ***remedy*** for his/her problem and ***compensation*** as appropriate? What is the procedure?

- **mandatory external audits**. How often are they carried out?

- "**appropriate [and effective external] supervision** of the relevant services' activities"

  Note: This supervision should "normally" be carried out by the judiciary. If it is not, there should be particularly strong alternative supervisory mechanisms, such as close Parliamentary scrutiny (cf. the Klass- and Kopp-judgments of the EuCtHR, referred to in its Rotaru-judgment). What are the specific arrangements? What is the role of the Information Commissioner? Can he refer appropriate cases to the courts?