fipr

Children's Databases – Safety and Privacy

A Report for the Information Commissioner

Foundation for Information Policy Research

Ross Anderson
Ian Brown
Richard Clayton
Terri Dowty
Douwe Korff
Eileen Munro

Final version

About the Authors

Ross Anderson chairs the Foundation for Information Policy Research. He is Professor of Security Engineering at Cambridge University, a Fellow of the IEE and the IMA, and a pioneer of the economics of information security.

Ian Brown is a senior research manager at the Cambridge-MIT Institute and a researcher at UCL, with a PhD in information security. He is a member of the Advisory Council and a former Director of the Foundation for Information Policy Research.

Richard Clayton is a Trustee of the Foundation for Information Policy Research. He has a PhD in anonymity and traceability, and consults for the telecoms industry. He is also a research associate at Cambridge University Computer Laboratory.

Terri Dowty is Director of Action on Rights for Children. She has many years' experience in education and children's human rights. She sits on the Advisory Council of the Foundation for Information Policy Research.

Douwe Korff is Professor of International Law at London Metropolitan University. He has written extensively on data protection, including four reports for the European Commission. He also sits on the Advisory Council of the Foundation for Information Policy Research.

Eileen Munro is Reader in Social Policy at the London School of Economics. Formerly a social worker, her main area of research is child protection, with a particular focus on risk management. She sits on the Advisory Council of the Foundation for Information Policy Research.

Acknowledgements

We received help from a number of people including: Paul Whitehouse, Nick Bohm, William Heath, Lorna Brady, Michael Gould, Chris Andrew, Simon Grigor, Chris Hirst, Terry Keane, Terry Knowles, Susan Pickerill, Thilo Weichert, Holger Brocks, Lukas Gunderman, Thorsten Koop, Marie Georges, Leslie Basse, Norbert Fort, Ulco van der Pol, Bruce Adamson, Spike Cadman, Phian Davies, Ian Dowty, Elizabeth Forster, Mel Greenyer, Linda Kerr, Maire McCormack, Kathleen Marshall, Laura Paton, Claire Phillips, Sara Reid, Ann Stuart, Lucy Ruddy, Chris March, Peter Mucklow and Alan Cranston. We were also helped by a number of anonymous members of the teaching profession.

The URLs cited in this report were verified in March 2006 when it was delivered to the Information Commissioner. Some minor changes were made in August 2006 following feedback from affected government departments.

Chapter 1. Executive Summary

The Foundation for Information Policy Research (FIPR) was awarded a tender by the Information Commissioner to undertake a research project on 'identifying the growth in children's databases and assessing the data protection and privacy implications'. Its aim is to provide the Commissioner with a comprehensive view of current and proposed databases, particularly in the public sector, their extent, their role, and their potential effect on the privacy of individuals. It is also to provide an authoritative basis from which the Commissioner can develop his policy on data protection, and contribute more widely to the debate on this issue, and to public policy generally.

Background

The specific background to the project is the establishment recently of databases relating to children across social services, education, crime and health.

The Government is concerned that while crime generally is falling, there is a rise in violent crime – much of it committed by disadvantaged young people – and has launched a number of initiatives to be "tough on the causes of crime". These range from population-based measures, such as parenting classes and preschool provision under the 'Sure Start' program, to targeted measures such as the Youth Inclusion Programmes (YIPs). These operate in high-crime areas, in each of which the YIP targets the 50 or so children aged 13–16 deemed to be at greatest risk of offending.

Two distinctions are important here. The first is between 'child protection' (which relates to the 50,000 children in the UK believed to be "at substantial risk of significant harm") and 'child welfare' (which refers to perhaps 3–4 million children at some disadvantage such as poverty, ill-health or poor school performance). The second distinction is between measures taken for the benefit of the child and measures taken for the benefit of the community. In French, these are succinctly described by the words '*education*' and '*repression*'. Although this distinction is emphasised much less in the UK, it is also embedded in our law: measures undertaken for general social benefit rather than for the direct benefit of the subjects must often meet tougher data-protection criteria.

While the scope of child social work in the UK has always included child welfare, its dominant focus in recent years has been child protection. Policy is now to broaden that focus to place more emphasis on welfare, and also on crime prevention. There is also a strong push from the e-government agenda – the notion that computerisation can be used to drive changes in public-service organisation and professional working practices.

In order to target preventive measures more accurately, the Government seeks to collect information relating to risk factors from a wide range of public services. This ranges from personal medical information (such as early diagnoses of hyperactivity) through school results, social workers' casenotes, and information from police and youth-justice systems. The development follows the same general lines as the computerisation of the NHS: there

will be a central register, ISA, recording the public services with which a child has had contact, and a system of electronic social-work casenotes similar to the NHS Care Records Service. A number of systems supporting various kinds of youth work, youth justice and surveillance are also under development.

Problems

One concern is what we might call ‘e-discrimination’. In the past, it has been well documented that children who were black, or from poor neighbourhoods or travelling families, suffered disproportionate police attention because of the expectation that they would be more likely to offend. The expectation could easily turn into a self-fulfilling prophecy. A system that attempts to predict which children will become delinquent, by totting up negative indicators from health, school and other records, runs the serious risk of recreating the same problems – especially as the information, analysis and professional opinions it contains will be made available to many of the public-sector workers who come into contact with the child. A perfectly law-abiding youngster from a difficult home background, who has perhaps struggled to overcome learning and health difficulties, may find at every turn that teachers expect less, and that police attention is more likely. As the causes of this discrimination are online, the youngster cannot mitigate them simply by dressing neatly and being polite. The data and algorithms used as a basis for discrimination might not be accessible to the victim (whether practically or at all) and thus a victim of unjustified discrimination might end up with no recourse. This raises serious data protection concerns relating to the appropriateness of collecting, processing and retaining the data.

A second bundle of concerns relate to the scarcity of effective social interventions. The privacy intrusion attendant on (say) a cervical cancer screening program may be quite justified by the lives saved. However, delinquency is less tractable than cancer. Both of the government’s flagship intervention programmes – Sure Start and the YIPs – have had, at best, mixed reviews for their pilot stages. It is also well known that the effectiveness of social intervention programs tends to fall when they are rolled out from the experimental or pilot stage to become nationwide policy, and so we may expect that their effectiveness will fall still further. There is thus less justification for privacy intrusions than would be the case for example with a traditional public-health initiative.

Our third bundle of problems concern a rather cavalier interpretation of data protection law and privacy law by a number of the agencies involved in building the network of children’s databases. For example, the Gillick precedent (confirmed recently in the Axon case) establishes that a child’s parents should normally be involved in matters of consent, but that, exceptionally, the child may exercise the consent function to the exclusion of the parent if he or she insists on it and has the maturity to understand the consequences. This has been routinely turned into a principle that anyone over 13 can consent to sharing sensitive personal information without the involvement of their parents. In some circumstances the consent is obtained coercively, with implied threats of loss of access to services. This is unlawful. Another example is the proposed collection of information on sexual activity of 16–18 year olds, in the name of child protection, even though such persons are over the age of legal consent. This breaches human-rights law. A third

example we found was police sharing data on a 9-month-old baby without the parents' consent using the excuse of 'crime prevention'. To be fair, many of these abuses stem more from ignorance than from malice. There is plenty of opportunity for the Information Commissioner to educate, to warn, and to take enforcement action.

Our fourth bundle concerns the actual harm that sharing can do. Government documentation and guidance is mostly unbalanced in that it ignores the dark side; it pays little heed to family values, therapeutic effectiveness, trust and privacy. By failing to respect the users of the social-care system, it risks deepening rather than ameliorating social exclusion. There is specific harm: in a disturbing recent case, a nine-year-old was wrongly taken into care after social workers misunderstood medical information. Increasing the amount of poor-quality data available will lead to more errors, and out-of-context information can easily cause risk-averse staff to panic, with serious consequences. There are also institutional and professional risks. US information-sharing pilots have in many cases shown negative outcomes, because of the diffusion of responsibility; and recently, professional disquiet in the UK has led to the `Social Work Manifesto' whose authors object to having to "collude with youth justice policies which demonize young people".[1] Even if one does not share this radical view, there are certainly growing problems of recruitment and retention within the profession.

Nor is the criminal-justice community happy. Britain's most eminent criminologist, Professor David Farrington FBA (whose work has been used extensively to justify the children's database program) sounds a warning note:

> *"Caution is, however, required. In particular, any notion that better screening can enable policy makers to identify young children destined to join the 5 per cent of offenders responsible for 50-60 per cent of crime is fanciful. Even if there were no ethical objections to putting "potential delinquent" labels round the necks of young children, there would continue to be statistical barriers. Research into the continuity of anti-social behaviour shows substantial flows out of – as well as in to – the pool of children who develop chronic conduct problems. This demonstrates the dangers of assuming that anti-social five-year-olds are the criminals or drug abusers of tomorrow, as well as for highlighting the undoubted opportunities that exist for prevention."* [2]

This report describes in detail the policy background, the systems that are being built, the problems with them, and the legal situation in the UK. An appendix looks at Europe, and examines in particular detail how France and Germany have dealt with these issues. Our report concludes with three suggested regulatory action strategies for the Commissioner: one minimal strategy in which he tackles only the clear breaches of the law, one moderate strategy in which he seeks to educate departments and agencies and guide them towards

[1] 'Social Work – A Profession Worth Fighting For?', Chris Jones, Iain Ferguson, Michael Lavalette, Laura Penketh, at http://www.liv.ac.uk/~swfuture/

[2] 'Support from the Start: working with young children and their families to reduce the risks of crime and anti-social behaviour', C Sutton, D Uttting, D Farrington, Home Office Research Brief RB524 (March 2005)

best practice, and finally a vigorous option in which he would seek to bring UK data protection practice in these areas more in line with normal practice in Europe, and indeed with our obligations under European law.

Chapter 2. Policy Background

The network of children's databases is commonly marketed as being about child protection – about preventing another Climbié case. However it actually represents a significant broadening of the focus of child social work from protection to welfare and from there to primary and secondary crime prevention. Its development has also been coloured by the e-government agenda. In order to understand this background, it may be as well to take things in their historical perspective.

In 1993, when Tony Blair became shadow Home Secretary, he adopted the slogan "tough on crime, tough on the causes of crime". This focus on the causes of crime, and of other social problems, lies at the heart of policy for children's services. Prevention rather than cure has obvious attractions, and the case was strengthened by research that increased understanding of why some children developed problems. The factors that were associated with poor outcomes for children were listed in the 2003 Green Paper Every Child Matters as:

- low income and parental unemployment
- homelessness
- poor parenting
- poor schooling
- postnatal depression amongst mothers
- low birth weight
- substance misuse
- individual characteristics, such as intelligence
- and community factors, such as living in a disadvantaged neighbourhood.

It is important to note that these factors are neither necessary nor sufficient to lead to crime or other poor outcomes. Many children will overcome the experience of these adverse factors and many criminals, especially those guilty of white collar crime, did not experience them. The limited predictive value of risk factor research means that the group of children who will develop significant problems cannot be accurately picked out: 'Children at risk do not form a self-contained, easily defined group'.[3] At best, one can identify a group with higher than average probability of developing problems, but many in the group will not do so, whether or not special help is offered, and many children outside the group will, in fact, turn out to be problematic. The limitations of predictive research have led to a major debate in the preventive literature about the relative merits of universal versus targeted services for reducing problems.

[3] HM Treasury, 2002, 'Spending Review. Opportunity and Security for All: Investing in an enterprising, fairer Britain', para 28.3

2.1 Primary Prevention of Problems

The modern approach to crime prevention is based on the belief that offending is just a symptom of a larger syndrome of antisocial behaviour, and that the benefits of a crime prevention programme can be broader, spilling over, for example, into education. Some studies and pilot projects, especially in the USA (where the 'Head Start' program has been running since 1965), have strongly suggested that offending can be reduced by giving poor, single teenaged mothers antenatal and/or postnatal visits from nurses to educate them in parenting, and by providing free day care.[4]

The next questions concern the nature and level of service provision. Should we improve health-visitor services everywhere or concentrate on deprived areas? Should preschool education be a universal right, like primary education, should it be targeted on needy areas, or should it be means-tested?

Epidemiologists – notably the late Geoffrey Rose – studied the circumstances in which it is most efficient to treat the 'high-risk' cases or the whole population.[5] With some diseases, targeting makes sense, while with others it is not efficient. Problems such as alcohol abuse, obesity and hypertension have a complex mixture of causes (genetic, developmental, and cultural) and their incidence exhibits what statisticians call a normal distribution. It is possible to predict the number of problem drinkers in a country from the per capita alcohol consumption, the incidence of hypertension from the average blood pressure, and so on. The deviant 'tail' is a manifestation of the underlying distribution and remains about the same size, but whether or not the individuals within this tail pose a significant problem will depend upon the median incidence for that society. With problems that have this property, population-based preventive strategies can generally be expected to be more effective. This is especially so where the problem reflects socially-conditioned lifestyle choices. As Rose remarked:

> *"It makes little sense to expect individuals to behave differently from their peers; it is more appropriate to seek a general change in behavioural norms and in the circumstances which facilitate their adoption."*

This may now be uncontroversial in the case of smoking, where policy is to change social norms; we use taxation and workplace smoking bans rather than a national register of nicotine addicts. Should it also be the case for delinquency? One might argue, for example, that a population somehow 'treated' so as to become less aggressive might have fewer criminals, but also fewer Nobel Laureates and fewer world-class businessmen.

Criminological research suggests that children normally learn to control and channel their aggression by the time they enter primary school, and are helped to do so by parents who set and enforce consistent rules. Some children do this less well, and indeed aggressive behaviour exhibits a normal distribution. It is more common in 'problem' families, and

[4] RE Tremblay, C Japel, 'Prevention during pregnancy, infancy and the preschool years' in DP Farrington, JW Coid (eds) Early Prevention of Adult Antisocial Behaviour, CUP (2003).
[5] G Rose, 'The Strategy of Preventive Medicine', Oxford University Press (1992)

tends to persist; disruptive toddlers are more likely to acquire criminal convictions later. There may thus be a case for early intervention. But should this be targeted at problem families, or offered to all? The data are not quite as clear-cut as with alcohol or hypertension. Cost-benefit analyses of US delinquency-reduction programs show a positive benefit in five studies, an inadequate return in two more, and one in which the return was positive only for the high-risk families.[6] It should be noted that the US Head Start programs are generally restricted to low-income families, and that the measured benefits include higher income and welfare-cost reduction as well as the public and victim benefits of crime reduction. Overall, though, experts believe that a population strategy is justified.[7]

This is the background for 'Sure Start', originally described as "a cornerstone of the Government's drive to reduce child poverty and social exclusion". Its strategy was to set up pilot projects in a number of deprived areas. These projects provided pre-school education for 3–4 year-olds as well as integrating with health-visitor and primary-care services. The goal was to establish the programme and then roll it out nationwide. Each local programme caters for 400–800 children, and is run by a board with representatives from education, social services and health, plus voluntary organizations and parents.

Assessments of Sure Start have, however, been a disappointment. The initial evaluation in June 2002[8] focused on early implementation problems, while the first substantive evaluation in July 2005[9] showed that (compared with the rest of England) the Sure Start pilot areas showed an increase in social work activity; of benefit uptake; and of children being assessed as having special educational needs. A slight increase in immunization, and a slight fall in fertility, indicated better engagement with health services. The pilot areas also exhibited stronger economic and employment growth than England as a whole. Thus the 'input' factors – social, medical and economic – are all up. However, the key outcome indicators have been disappointing. Average birth weights are down, while neonatal and infant mortality are up. There is also a perception that the most needy families get little benefit, and may even suffer adverse consequences.

The question now is whether Sure Start has been doing the wrong things, or doing them wrong, or whether it's simply too early to see the benefits. Some researchers are also becoming disillusioned, believing Government to be more interested in avoiding criticism than in learning from policy and implementation mistakes.[10]

---

[6] BC Welsh, 'Economic costs and benefits of primary prevention of delinquency and later offending: a review of the research', in DP Farrington, JW Coid (eds) Early Prevention of Adult Antisocial Behaviour, CUP (2003), pp 318–335

[7] JW Coid, 'Formulating strategies for the primary prevention of adult antisocial behaviour: 'high-risk' or 'population' strategies?', in DP Farrington, JW Coid (eds) Early Prevention of Adult Antisocial Behaviour, CUP (2003), pp 32–78

[8] J Tunstill, D Allnock, P Meadows, A MacLeod, 'Implementing Sure Start', at http://www.surestart.gov.uk/_doc/P0000405.pdf, accessed 18 February 2006

[9] J Barnes, C Desousa, M Frost, G Harper, D Laban, 'National evaluation report – Changes in the Characteristics of Sure Start Local Programmes Areas in Rounds 1 to 4 between 2000/2001 and 2002/2003' at http://www.surestart.gov.uk/_doc/P0001726.pdf, accessed 18 February 2006

[10] T Hope, 'Things can only get better', CJM no 62 (Winter 2005-6), Centre for Crime and Justice Studies, pp 4–5 and 39

Secondary Prevention to Stop Problems Getting Worse

Improving universal services and developing new ones for the early years may prevent the emergence of problems in some children. The next level of prevention, however, is to respond when children show low-level signs of difficulty with the aim of preventing these escalating into less tractable problems. The main driving force behind the need to collect and share information on children is the goal of identifying those who are displaying early signs of problems. This, it is hoped, will lead to provision of help, and this help will be effective in solving the problems so that the child does not become problematic and is able to fulfil his or her potential.

This represents a major change in social care policy. While Britain provides some universal services to all children, such as health and education, policy has otherwise favoured a residual, reactive approach to state intervention in family life. Child and family social workers (created by the 1948 Child Care Act) have historically intervened in very few families (mainly of low income), offering a range of support services to prevent children coming into public care, or to support children with disabilities, and providing alternative care for those few children who could not be cared for by their birth family. In 1968, the Seebohm Report led to the integration of social work services so that 'families' rather than individuals were the target for help, reducing the number of professionals working with one family and recognising the interconnectedness of family members. Since the 1970s, social services have been overwhelmed by referrals about child abuse as it has become a prominent public concern. The public and professionals have been urged to refer any suspicion that a child is being abused or neglected, leading to a steep rise in the number of allegations that are investigated. However the number of substantiated cases of abuse causing 'significant harm' (a legal category) has not risen to the same extent. 75% of referrals are not considered serious enough to warrant a case conference. Overall, the majority of families referred and investigated receive no help.[11]

A series of highly public inquiries into the deaths of children from abuse have shaped the priority given to referrals about abuse, with workers in all services worried about missing a case of serious abuse. Consequently, the resources available for other children's services have been reduced. Families with low-level concerns are turned away, and only receive help if the problems escalate to a level where they can be categorised as abuse. For example, the mother of a child with severe physical disabilities may say she is getting to the end of her tether and ask for more support, but may not get extra help until she loses her temper and hits the child.

The skew towards investigation of abuse also affects the assessment of and response to the families investigated. Inquiries tend to be focused on whether or not abuse has occurred and whether the child is at risk of significant harm. Consequently, the assessment misses the child's wider needs, although most children investigated are clearly living in stressful circumstances. In terms of response, shortage of therapeutic resources means that families in which abuse is substantiated often get little help.

[11] J Gibbons, S. Conroy. C Bell (1995) Operating the Child Protection System: A Study of Child Protection Practices in English Social Services. London, HMSO

Between a quarter and a third of all known victims of abuse are estimated to suffer re-abuse. Even children who have been abused receive little assistance: only 6% of victims of sexual abuse get therapeutic help. This state of affairs has worried people for a long time.

Many of the families screened out of the system are clearly struggling with low incomes, mental health problems, domestic violence etc. They may not be abusing their children at present, but the circumstances are such that the risk of future abuse is higher than average. Moreover, these are adverse factors for children's health and development whether or not they provoke parental abuse or neglect. Criminological and epidemiological research (summarized above) argues for broad provision rather than simply targeting abuse cases. There is also a moral argument for minimising the time a child suffers some problem, and for providing help to non-abusive mothers and fathers who are struggling with their parenting responsibilities. Also, if professionals could refer families for help from non-abuse services, they would remain visible to the system and missed cases of abuse would thus be more likely to get spotted.

Both Conservative and Labour governments have sought to shift the balance of work in children's services. In the Children Act 1989 the Conservative government attempted to put more emphasis on supporting families and keeping the policing and coercive elements of child protection work to a minimum. However, the legislation sets out a power to provide family support (Section 17) and a clear duty to investigate allegations of abuse (Section 47) and priority continued to be given to meeting Section 47 duties as the social and political pressures continued to prioritise abuse. In the mid 1990s, considerable effort was put into encouraging children's services to 're-focus' their efforts and give more attention to supporting families who were living in difficult circumstances.[12] Progress on this has been slow, however, and government research found that local authority social services departments had found it difficult to implement the policy since dealing with allegations of abuse continued to absorb so much of their resources.[13]

The case of Victoria Climbié, who died in 2000, illustrates some of the adverse effects of this bias in service provision. The referrals about her were classified as Section 17 (needing support) not Section 47 (requiring investigation). Therefore little help or attention was offered to her or her great-aunt. Hence, she could be known to a large number of services but all felt justified in having limited involvement, despite it being obvious that she was living in circumstances that were unlikely to help her grow into a happy and healthy adult.

2.2 The e-Government Agenda

Throughout the 90s there was growing recognition throughout the European Union that developments in IT were bringing irrevocable change to world economies, to governance

[12] Dept. of Health, 1995, Child Protection: Messages from Research. London, HMSO
[13] Dept. of Health, 2001, The Children Act Now: Messages from Research, London, The Stationery Office

and to society as a whole. By March 2000, EU heads of state meeting in Lisbon had agreed a strategy that would harness IT in the service of making the EU: *"the most competitive and dynamic knowledge-driven economy by 2010"*.

A cornerstone of what was named the 'Lisbon Strategy' was the development in each EU country of government service delivery by electronic means. It was envisaged that electronic service delivery, or 'e-government', would offer citizens faster and more efficient services, while also stimulating the IT market by fostering demand for new products. As an EU Communication on the strategy explained:

> *"The world economy is moving from a predominantly industrial society to a new set of rules – the information society. What is emerging is often referred to as the new economy…*
>
> *"The underpinning dynamics of the new economy are strong. Digital technologies make accessing, processing, storing and transmitting information increasingly cheaper and easier. The sheer scale of information available creates huge opportunities for its exploitation through the development of new products and services. Transforming digital information into economic and social value is the basis of the new economy, creating new industries, changing others and profoundly affecting citizens' lives."* [14]

In the UK, the Government had already begun work on its manifesto promise of modernisation. July 1998 saw both the creation of the Performance and Innovation Unit within the Cabinet Office, and the publication of the White Paper: Modern Local Government: in Touch with the People.[15] This was a consultation paper for the Local Government Act 2000, which paved the way for 'joined up' local service delivery.

In December 1998, the White Paper: Our Competitive Future: building the knowledge-driven economy[16] announced the Government's intention to *"appoint a Special Representative for the Digital Economy (the e-Envoy)"*.

In 1999 the Government produced a further White Paper, Modernising Government,[17] that outlined plans for *"joined-up government in action"* and proposed targets for the electronic delivery of public services.

This was followed in April 2000 by the publication of the Cabinet Office strategy document: e-government[18] that fleshed out the White Paper's ideas and said:

---

[14] e-Europe: An Information Society For All
http://www.e-europestandards.org/Docs/eeurope_initiative.pdf
[15] Modern Local Government: In Touch with the People White Paper 30/7/98 Command No. 4014
[16] Our Competitive Future: building the knowledge-driven economy
http://www.dti.gov.uk/comp/competitive/main.htm
[17] 'Modernising Government' 30 March 1999
http://www.archive.official-documents.co.uk/document/cm43/4310/4310-00.htm
[18] e-government: A Strategic Framework for Public Services in the Information Age
http://archive.cabinetoffice.gov.uk/e-envoy/resources-pdfs/$file/Strategy.pdf

> *"New technology offers opportunities for sharing data between departments in support of integrated services…The Government will continue to consider whether further legal provision is needed to provide for data sharing in support of these objectives."*

The Cabinet Office's Performance and Innovation Unit was tasked with looking at ways in which 'e-government' could be taken forward. Their first e-government report, Wiring it up,[19] in January 2000, examined the potential for 'cross-cutting' working across central government. This report was followed in September 2000 by: Electronic Government Services for the 21st Century,[20] which set out a strategy for *"realising the full potential of electronic service delivery"*.

A further report from the PIU in April 2002, Privacy and Data-sharing,[21] outlined the key areas in which the Government could make rapid progress in developing e-government. In particular, Chapter 11 of the report recommended as an objective the early identification of children, young people and their families at risk of social exclusion: *"Local agencies need to be able to identify quickly children at risk of social exclusion and provide the support they need to keep them on track"*. Information sharing would allow agencies: *"to build up a holistic view of children's needs, and ensure children do not slip through the net"*.

FAME

The Office of the Deputy Prime Minister has funded a number of projects to take forward the e-government agenda set out in their National Strategy for Local e-Government[22] and the White Paper Strong Local Leadership – Quality Public Services.[23] The most significant of these for the development of multi-agency sharing of personal data is the Framework for Multi-Agency Environments (FAME) project,[24] based at Newcastle University.

FAME is developing a framework for multi-agency information sharing, and is working with local and regional agencies to implement this framework in their information systems. The boundary for the sharing of information is not at the local-authority level: larger agencies such as Primary Care Trusts may also participate fully.

---

[19] Wiring it up: Whitehall's Management of Cross-cutting Policies and Services Cabinet Office Performance and Innovation Unit January 2000 Ref: CABI 99-5265/0001/D16

[20] e-gov: Electronic Government Services for the 21st Century Cabinet Office Performance and Innovation Unit September 2000 Ref: CABI 00-6374/0009/D24

[21] Privacy and data-sharing: The way forward for public services Cabinet Office Performance and Innovation Unit April 2002 Ref: CABI J01-9063/0402/D16

[22] e-gov@local: towards a national strategy for local e-government: consultation Office of the Deputy Prime Minister 2002 http://www.odpm.gov.uk/index.asp?id=1137926

[23] 'Strong Local Leadership – Quality Public Services' Office of the Deputy Prime Minister December 2001

[24] http://www.fame-uk.org/

The project's major concern has been to find ways in which agencies can share information to improve the delivery of services, particularly in areas where this has proved difficult in the past. The framework has been designed to be flexible and to allow reshaping in response to changing requirements. Its core services revolve around identity, consent and geography, although the consent functionality is so far relatively undefined – not least because relatively little work has been done in this area by local and regional authorities. A central publication and collaboration space lists agencies that have information about specific individuals, which must, if required, be requested through that agency rather than directly shared.

The project's overall aim is to support practitioner decisions rather than to supplant their professional judgment. The initial funding ends in April 2006, but will be continued from other local government sources.

2.3 From Protection to Safeguarding

Collecting and sharing data on children is now seen as crucial to improving children's well-being:

> *"A positive commitment to information sharing between professionals and agencies, taking full advantage of the opportunities set out under statute, is the only way to ensure that all children and young people are provided with the most appropriate support as and when they need it."* [25]

It is important to be clear about the distinction between the government's broad policy goal of 'safeguarding children' and the narrower focus of 'child protection', since they pose different data protection issues.

'Safeguarding' covers all the problems of childhood and is defined by the government as:

> *"The process of protecting children from abuse or neglect, preventing impairment of their health and development, and ensuring that they are growing up in circumstances consistent with the provision of safe and effective care which is undertaken so as to enable children to have optimum life chances and enter adulthood successfully."*

This comes from a standard DfES reference,[26] which was the subject of extensive consultation, and which also gives the following definition for child protection:

> *"The process of protecting individual children identified as either suffering, or at risk of suffering, significant harm as a result of abuse or neglect"*

[25] DfES, op. cit., 2003, p.2
[26] Working Together to Safeguard Children, DfES, 2005, p. 11

Child protection, therefore, is specifically concerned with (a) abuse or neglect (also referred to as 'child maltreatment' in government documents) and (b) harm of a severity to be called 'significant'.

It is crucial to keep this distinction between child protection and safeguarding (or welfare, as it is often referred to) clear throughout the following report, since the two areas of work present substantially different data protection issues. Since the death of Maria Colwell in 1973, it has become a primary principle in children's services that information about a family needs to be shared, with or without consent, when there are child protection concerns (DHSS, 1974).[27] By sharing their individual perceptions of a family, workers are able to construct a more accurate and comprehensive picture of family functioning and the child's safety and well-being. Sharing information without consent may be both necessary and justified in this context because abusive parents may go to extreme lengths to conceal their wrong-doing. All the main professional groups have made it clear that child protection concerns can override any principle of confidentiality, e.g. General Medical Council, 2004, para.27, and this is also clear in the Data Protection Act 1998. To facilitate good information sharing, Local Children's Safeguarding Boards (previously Area Child Protection Committees) publish procedures to give workers clear information about how and with whom to share their child protection concerns.

No-one disputes the importance of professionals sharing information in child protection cases but the government's new safeguarding agenda proposes that it is also crucial in tackling all other childhood problems. The central role ascribed to information sharing is the result of a number of policy changes, both in relation to how government operates in general and with specific reference to children's services. This chapter began by examining the importance of data collection in developing e-government and in modernising public sector services. Children's services are part of this wider agenda but policy here has also undergone fundamental change, with a new emphasis on government taking an active, interventionist approach to family life in order to prevent problems developing. The way in which the government has chosen to pursue the goal of prevention is fundamentally changing the relationship between families and the State. It has created a managerial framework for children's development, with an audit system of targets and performance indicators. Responsibility for achieving the targets has been given to professionals in children's services and this, consequently, leads to a fundamental reduction in the autonomy and privacy of family life.

2.4 "Every Child Matters"

The most recent approach to children's policy, embodied in the 2003 Green Paper: Every Child Matters: Change for Children[28] (hereafter referred to as ECM) continues this drive to develop preventive and support services. The 2002 Spending Review by HM Treasury had found that: "despite extensive investment in services for children, most services are

[27] DHSS (1974) Report of the Committee of Inquiry into the Care and Supervision Provided in Relation to Maria Colwell. London, HMSO.
[28] See for example www.everychildmatters.gov.uk/aims/background; accessed December 6th 2005

not having the desired positive impact on the most disadvantaged children".[29] The ECM Green Paper made a strong case for change:

> *"We need to shift away from associating parent support with crisis interventions to a more consistent offer of parenting support throughout a child and young person's life. We will work towards a mix of universal and targeted parenting approaches, including advice and information, home visiting and parenting classes"* (para 3.6)

The Prime Minister, Tony Blair, summed up the political drive behind the policy in his introduction to the Green Paper:

> *"This country is still one where life chances are unequal. This damages not only those children born into disadvantages, but our society as a whole. We all stand to share the benefits of an economy and society with less educational failure, higher skills, less crime, and better health. We all share a duty to do everything we can to ensure every child has the chance to fulfil their potential."*

The four key themes were summarized as:

1. Increasing the focus on supporting families and carers – the most critical influence on children's lives

2. Ensuring necessary intervention takes place before children reach crisis point and protecting children from falling through the net

3. Addressing problems identified in the report into the death of Victoria Climbié – weak accountability and poor integration

4. Ensuring that the people working with children are valued, rewarded and trained (this is to deal with the serious problems in recruitment and retention of staff that have developed in the last ten years).

The scope of children's services has been dramatically widened. The Government's aim is for every child, whatever their background or their circumstances, to have the support they need to:

- Be healthy
- Stay safe
- Enjoy and achieve
- Make a positive contribution
- Achieve economic well-being

[29] HM Treasury, 2002, Spending Review. Opportunity and Security for All: Investing in an enterprising, fairer Britain, para 28.4

The success of children's services in achieving these five targets will be measured by a complex set of performance indicators.

The shift from universal to targeted services, where the need for additional help is identified by professionals rather than parents, creates the drive for extensive data collection so that agencies can build up a wide-ranging picture of a child's functioning.

The key data collection systems (discussed in more detail in Chapter Three) will be:

CAF – the common assessment framework to be completed by any professional when they consider that a child has additional needs that require the involvement of more than one service. The idea is to save time by doing one assessment that can be used thereafter. It is a wide-ranging set of data covering every aspect of a child's health and development, including details about the parents and siblings. The reliability and validity of the data will be a crucial factor in determining whether professionals make use of it.

ISA or **IS** – Information Sharing (and Assessment) Index, containing basic details of all children in England, including all professionals in contact with them and their contact details. (This is beginning to be referred to simply as IS.)

ICS – a system for children's social services that will include the case records of all children known to social workers. The extent to which information on this database will be linked to the systems in health, education, and criminal justice is not yet clear.

The Role of the Education Service in ECM

Education is central to government policy, not just in terms of producing a skilled workforce, but also to the reform of children's services, to poverty-reduction strategies and to the wider 'Modernising Government' agenda. The envisaged function of education and schools in the delivery of government policy can be briefly summarised as:

- Ensuring that children have the skills to equip them for future work
- Providing a vehicle for long-term social change
- Monitoring attainment and behaviour in order to identify social problems
- Delivering services to children and young people

The 1999 White Paper: Learning to Succeed, emphasised the urgent need for educational change:

> *"The skill needs of the future will be different from those of today and it is clear that we will not keep pace with the modern economies of our competitors, if we are unable to match today's skills with the challenge of the developing information and communication age of tomorrow. As labour markets change, we*

must develop a new approach to skills, and to enabling people, and businesses, to succeed." [30]

At the same time, the Social Exclusion Unit published a report, Bridging the Gap,[31] that identified as a problem the fact that around 161,000 young people aged 16–18 were not engaged in education employment or training (NEET). The response to these concerns was the establishment of the 'Connexions' service for 13-19 year-olds, which had the aim of encouraging participation in education, and dealing with personal problems that might present "barriers to learning". The model was one of a multi-agency team that shared information about the young person, co-ordinated by a key worker: the Connexions Personal Adviser.

The Connexions model enabled the identification of young people who were "disengaged" from education, and also those whose difficulties matched the criteria for determining a risk of future offending behaviour. The Connexions PA could then broker access to appropriate services.

Connexions embodies the growing interest in the 'risk management' of children; in other words, identifying factors that might lead to later problems in order to offer early intervention. Schools provide a ready environment for conducting such assessments: challenging behaviour at school – or absence from school – are seen as indicative of a likelihood of committing criminal offences in the future. Lack of educational achievement and aspiration are viewed as predictive of a range of problems, including unwanted teenage pregnancy. Educational attainment is seen as a crucial tool in combating poverty, deprivation and social exclusion.

The Every Child Matters agenda proposes a substantial shift in the traditional role of schools. The vision is of:

> *"promoting full service extended schools which are open beyond school hours to provide breakfast clubs and after-school clubs and childcare, and have health and social care support services on site"* (ECM Executive Summary, page 7)

Thus the future school is seen as a community hub, where education is one of a number of services working together to provide childcare from 8am to 6pm, oversight of children and their families, and a complete package of health and social care.

Child Protection

Alongside the concern to reduce crime, anti-social behaviour, under-achievement at school, and teenage pregnancies, the government wants to improve the child protection system that should help children who are at risk of significant harm from abuse. Lord

[30] 'Learning to Succeed: a new framework for post-16 learning' HMSO June 1999 http://www.lsc.gov.uk/National/Documents/SubjectListing/CorporateandStrategic/Corporate/'LearningtoSucceed'WhitePaper.htm

[31] http://www.socialexclusionunit.gov.uk/page.asp?id=53

Laming's report[32] into the death of Victoria Climbié came out shortly before the publication of Every Child Matters and illustrated many deficiencies in the services provided to children at risk of abuse.

The ECM agenda, emanating from the Home Office and HM Treasury, was not primarily aimed at abuse victims but includes them as one vulnerable group. The Climbié case has been seen as providing justification for the sharing of information and the development of computer databases to achieve this more efficiently. Indeed, some people mistakenly believe that the IS Index arose from analysis of the defects in Victoria's care. However, the plan to establish what was initially referred to as an Information, Referral and Tracking system (IRT) had already been announced by John Denham, Minister for Children and Young People at the Home Office in August 2002. It was intended to identify children at risk of offending, drug taking and teenage pregnancy.

The Laming Report did reveal major problems in practice but these lay mainly in the quality of the judgements and decisions made: that is, they showed poor professional expertise. The practitioners in contact with Victoria knew of each other's involvement and shared considerable amounts of information. The crucial errors arose from individuals either not paying attention to the information, or giving it a benign interpretation so that the risk to Victoria from abuse was not seen.

This is consistent with the finding from a review of child abuse inquiries; the nature of criticisms of practice has altered as the procedures for professionals working together have become well established. Criticisms that information had not been shared were common in inquiries undertaken in the 1970s, but became much rarer in later reports. They were replaced by criticisms that the information had not been accurately assessed.[33] That professionals often lack expertise in interpreting information is highlighted by the government in the draft Working Together to Safeguard Children,[34] the key guidance on inter-professional working. Chapter 8 ("Lessons from Research and Inspection") notes:

> *"Practitioners experience difficulties in analysing the information gathered during the assessment, consequently plans and services do not always relate to the child's developmental needs. Some children are not being properly safeguarded from harm; others are denied access to family support services."* (para.8.22)

If one of the core problems in accurately identifying children who are suffering, or are at risk of suffering significant harm, is the level of professional expertise in understanding data (rather than a lack of data per se), then providing more data does not seem to be the most obvious strategy for improving practice. In fact it may be counter-productive. If there is more data, time will be spent on absorbing it rather than acting upon existing

[32] H Laming (2003) *The Victoria Climbie Inquiry.* London, The Stationery Office.
[33] E Munro (1999) 'Common Errors of Reasoning in Child Protection'. Child Abuse and Neglect: The International Journal, 23:745-758
[34] Department for Education and Skills (2005a) Working Together to Safeguard Children – Draft for public consultation. London, HM Government

data. Additionally, important data may be hidden below insignificant data – this problem is well understood by those responsible for running criminal investigations, particularly those in real time (such as kidnaps), with which section 47 cases may be compared.

Paving the Way for "Every Child Matters"

The ECM agenda is not the first attempt of government to improve information-sharing in order to promote co-ordination of services. Centralisation of electronic medical records started in 1992; it inspired much of the architecture used elsewhere in e-government, and provided an early taste of arguments over data protection, privacy and professional autonomy (we discuss health systems in Chapter 6 below). As noted above, the 1999 White Paper Modernising Government led to work by the Performance and Innovation Unit on ideas for electronic service delivery. It envisaged a single file for each person, separated by electronic gateways. Children's services were identified early on as a suitable arena for the development of this agenda.

In 2000 the Connexions service for 13–19 year-olds began. This involves sharing information across agencies; it built up a database of all 13–19 year-olds by requiring the information from LEAs. Where a young person is believed to need services, a 'Personal Advisor' carries out an in-depth assessment: the APIR process (Assessment, Planning, Implementation and Review), whose results are kept in a local database. There is more on Connexions in Chapter 3 below. It is significant in that it seems to have been a pilot for the larger ECM agenda; certainly the methods are the same. This view is strengthened by the transfer of Connexions' Chief Executive, Anne Weinstock, to the directorate of the DfES when the ECM green paper was published in November 2003.

2.5 The Rest of this Report

The next chapter examines the core database systems being developed to implement the ECM programme: the Connexions service, which has acted as a pilot over the last few years; the new Information Sharing and Assessment index (ISA) – the national index of all children; the Common Assessment Framework (CAF) – to be used by all professionals in making referrals; and finally the Integrated Children's System (ICS) – the case management system for social care, where the CAF data will be stored.

Chapter 4 looks at the education databases run by the Department for Education and Skills (DfES). In parallel with the development of Connexions, the government introduced the National Pupil Database (NPD) in order to create educational profiles of each child in a state-maintained school. It began collecting individualised information via the Pupil Level Annual School Census (PLASC) in 2000, and the amount of information required has grown each year. From 2006 it will be collected termly rather than annually. The NPD now incorporates the Qualifications and Curriculum Authority records on the attainment of pupils in public exams and Key Stage tests. We discuss NPD and PLASC in detail, and also review the consultation on Cross Government Guidance on Sharing Information on Children and Young People, an initiative that is being led by the DfES.

In Chapter 5, the systems being developed in youth justice are reviewed. The ASSET assessment tool, for example, uses a set of predictive factors to identify the subgroup of delinquents who are likely to re-offend. ONSET is being developed to predict which as-yet-non-delinquent children will become delinquent. The main focus of the chapter, though, is RYOGENS, a system that enables youth justice workers to share information about children with other professionals.

As mentioned above, we then summarise the relevant health systems in Chapter 6. This growing network of social work, school, justice and other databases relies on a number of Acts of Parliament and statutory instruments to authorize information sharing. We describe this regulatory framework in Chapter 7.

Finally in Chapter 8 we assess the UK's strategy from the viewpoint of data protection and set out some options for regulatory action.

Information sharing between professionals raises all manner of questions of ethics, consent, data protection, privacy, safety and human rights. Britain is not of course the only country facing these issues, and in order to provide some independent points of reference we discuss the approach taken in a number of other European countries in an appendix

Chapter 3. Core Systems

Most of the core systems in social care are still at the design and piloting stages so we begin this chapter by looking at the most developed system – the Connexions service for teenagers – before outlining the proposals for the Information Sharing Index (IS), the electronic Common Assessment Framework (CAF), and the Integrated Children's System (ICS).

3.1 Connexions

This service was established in 2000 for 13-19 year olds. Based on the former Careers Advisory Service, it has a higher aim of offering:

> *"a much better support service, founded around personal advisers, to guide young people through their teenage years and help them get around the problems that might stop them from making the most of learning."* [35]

Connexions' goal is also described as reducing the number of NEETs – young people Not in Education, Employment or Training (these numbers are still rising). Although the service applies to all young people over 13, its main target group is young people who are deemed to be at risk of social exclusion. It takes a proactive role in identifying them – obtaining data from the National Pupil Database (described in Chapter 4 below) and asking other services to notify it of vulnerable young people.

Legislative Basis

The Learning and Skills Act 2000 created Learning and Skills Councils, and paved the way for the new 'Connexions' service. Sections 114-122 of the Act provided for widespread information sharing between agencies involved with each young person. These sections were commenced on April 1st 2001, after the initial Connexions pilots.

Section 114 of the Act permits the Secretary of State for Education to provide services that *"…encourage, enable or assist [] effective participation by young persons in education or training"*. A young person is defined as someone aged 13-19.

Section 117 provides that learning establishments must supply any person or body involved in the provision of services with the name and address of a student and that of his/her parents, together with *"…information in the institution's possession about a pupil or student"*; however, a student over 16 or the parent of an under-16 can forbid the supply of any information other than names and addresses.

Section 119 permits the Secretary of State to supply information, including social security information, to *"any civil servant or other person"* involved in the provision of s114

[35] Social Exclusion Unit (1999) Bridging the Gap. London, Social Exclusion Unit

services. This allows for the provision of information held on Child Benefit or any other social security systems.

Section 120 permits the following to supply information to the Secretary of State or to *"any other person or body"* involved in the provision of s114 services:

a) a local authority
b) a Health Authority
c) the Learning and Skills Council for England
d) a chief officer of police
e) a probation committee
f) a youth offending team
g) a Primary Care Trust

During its passage through Parliament, the data-protection and privacy implications of the Learning and Skills Act were not debated. At committee stage in the House of Lords, Baroness Blatch asked whether the plans to share information raised data protection issues, and was assured by Baroness Blackstone for the Government that the Data Protection Act would be fully complied with. At committee stage in the House of Commons, the matter was not raised.

It may be that the effects of granting such information-sharing powers to the Secretary of State and to public bodies were not fully appreciated, because there was little understanding at that time of developments in information systems, the uses to which they could be put, and the potential they created for widespread information-sharing.

CCIS Database

Each Connexions service operates independently and is the data controller for their database. They aim to compile a database – Connexions Customer Information System (CCIS) – of all young people over 13 in their area. Connexions has a number of powers to request data from other agencies e.g. details of young people from the education database, claims for social security payments, revocation of any benefits, and attendance at 'Jobcentre Plus'.

The CCIS database includes:

- name
- address
- date of birth
- phone number
- gender
- ethnic origin
- relevant health information
- special educational needs statement where appropriate

- current status (in school/college, employed with/without training, unemployed, not known, not available for education/training, moved away)
- name of personal advisor
- type and date of contact (e.g. interview, telephone, email)
- names of contact workers for the young person, together with their organisation and contact details (subject to written consent where sensitive information may be disclosed via the type of organisation, such as a Drug Action Team, Youth Offending Team, or Social Services in the case of young persons in care.)

This information is considered to be the minimum necessary to:

a) identify an individual uniquely, and
b) enable personal advisers to co-ordinate provision of support.

Access to this data is available to all managers and delivery staff in Connexions, and some of their partner organisations.

APIR Database

A young person may choose to contact Connexions, or may be referred (with or without their consent) by someone such as a teacher or social worker. Their main contact will be with their Personal Adviser (PA). An adviser who believes that a young person needs services makes an assessment using the APIR document (Assessment, Planning, Implementation and Review). This is a wide-ranging assessment of their health and development, which helps the PA decide how to help them. The form is completed by the PA, based on interviews with the young person and on information from other sources. A young person can ask to see their APIR document, and it is standard practice for them to at least see the summary – because it is used by them both in their joint planning of what to do.

Issues covered include:

- physical health
- income
- housing
- social and community factors
- family history and functioning
- capacity of parents/carers
- risk of (re-) offending
- relationships within family and society
- attitudes and motivation
- identity/self-image
- aspirations

- life skills, key skills, and basic skills
- achievements and participation
- substance use issues, and
- emotional well-being.

This data includes factual information, sensitive information, and subjective judgements (e.g. about the young person's motivation). In the practice guidance, PAs are advised that they should record only facts on the APIR form, but it seems that many of the categories require subjective judgement (e.g. on the parents/carers' capacity or the young person's *"evidence of clear and realisable goals for the short and long term"*). Therefore it appears difficult for PAs to implement the guidance on sticking to facts alone.

The form also includes considerable data about other people – both family members and social contacts – which raises questions about whether their consent is needed to share such information. There seems to be no guidance on this issue.

The APIR document is stored electronically but is not shared with other agencies in its entirety. PAs make a professional judgement about which parts need to be shared with others in order to plan the best help for the young person.

Consent

(a) Parental role: discussions of consent, both to record and to share data, refer mainly to consent by the young person, not by their parents. It appears to be believed that if a young person is 'Gillick competent' then parental consent is not needed. One area's guidance, for example, explains the 'Gillick competence' test as meaning that *"children are considered competent to make decisions on their own behalf when they are capable of understanding fully the nature of what is proposed"*. See Chapter 7 for a full discussion of Gillick competence.

(b) Consent to recording data: practice guidance states that information should only be recorded with the agreement of the young person except, in certain circumstances, basic contact details received from another source.

(c) Consent to sharing data: the guidance on this varies. Three examples are given below.

Example (1) from guidance issued by central office of Connexions.

> *"It is important to note that consent will frequently not be the legal basis for sharing information about a young person. However, from a policy point of view it is seen as best practice to gain a young person's consent before sharing information about them."*

Example (2) from one Connexions service guidance document:

> ***Appendix A – Circumstances where disclosures may take place without breach of the Data Protection Act Principles***
>
> *The 1998 Data Protection Act permits the disclosure of information provided, it has been fairly obtained and processed (the individual has been clearly informed how their information will be used and disclosed).*
>
> *Disclosures can also take place under certain circumstances, where the data protection principles will not apply – under the Act's non-disclosure provisions. Reliance on these must be assessed on a case by case basis.*
>
> *The provisions are:*
>
> - *At the request of and with the informed consent of the individual concerned, or someone authorised to act on their behalf.*
> - *For the prevention or detection of crime, the apprehension or prosecution of offenders, and taxation purposes. Requests for information must be on a case by case basis and where failure to provide the information would prejudice these purposes. All requests and responses must be appropriately authorised and documented.*
> - *Where information is made available to the public by or under enactment.*
> - *Where the disclosure is required by law or by the order of a court.*
> - *Where a disclosure is made in connection with legal proceedings, for the purpose of obtaining legal advice, and establishing, exercising or defending legal rights.*
> - *Where there is risk of serious harm or threat or life.*
> - *For the purpose of safeguarding national security.*
> - *By order of the Secretary of State.*

Example (3) from a Connexions 'good practice' document:[36]

> *"It is not reasonable to give 'blanket' confidentiality for two main reasons: first, because the service to a young person may be considerably improved if information can be shared with other agencies, for example the school or social workers, secondly, for reasons of safety. On the first of these, it may need to be explained to a young person that they cannot be helped unless something of what they say is communicated to others."*

This third example seems to imply that service efficiency is a reason for breaching confidentiality and, even if consent is obtained by telling the young person that, unless they consent, they cannot be helped, it would not be 'informed' consent.

---

[36] 'Developing good practice in Connexions: Techniques and Tools for Working with Young People.' Connexions National Research and Evaluation Strategy, pp.10-11.Downloaded January 23, 2006

Retention: data is kept on the live system up to a young person's 20th birthday; it may be their 25th if they have Special Educational Needs or LDD (Learning Difficulties and/or Disabilities). Data is archived for three years after the end of the financial year in which the young person turns 20 (or 25).

Future developments: the APIR document is similar in purpose and scope to the planned Common Assessment Framework (CAF). It is expected that Connexions will adapt their APIR form to include the elements of CAF but retain some distinctive categories specific to their needs. When the APIR becomes an equivalent of the CAF, then the issues raised in that section of this report about sharing information will apply.

3.2 Information Sharing and Assessment Index (IS)

This is a new national database, established under Section 12 of the Children Act 2004, which will contain data on all children in England, and should be fully operational by the end of 2008. This is a devolved matter, so that this system will only operate in England at the present time. Wales is considering a similar system, but has made no progress so far. Scotland has a parallel development but will implement a different type of index. In Northern Ireland, Education and Social Care is centralized, and a similar system is not expected. The database was originally called an 'Information Hub' as part of the 'Identification, Referral and Tracking' (IRT), then 'Information Sharing and Assessment' (ISA), and is now referred to as the 'Information Sharing Index' (IS) as part of the information sharing and assessment programme.

The English database is under development by the DfES, and we were able to talk with the officials involved and understand how they expect it to operate. Once it becomes operational, it will be operated as a single national database by the 150 Local Authorities who will be responsible – as data controllers – for the data on the children in their particular area.

The index is a key element of the Every Child Matters programme to transform children's services by supporting more effective prevention and early intervention. The index is seen as a tool to support better communication among practitioners across education, health, social care and youth offending. It is claimed that it will allow them to contact one another more easily and quickly, so that they can share information about children and young people who need services or about whose welfare they are concerned. The government estimates that, at any one time, 3-4 million children of a total population of 11 million have additional needs that may need action if the children are to achieve the outcomes set out for them in Every Child Matters.

The stated objectives of the index are to:

- help practitioners identify quickly a child with whom they have contact, and whether that child is getting the universal services (education, primary health care) to which he or she is entitled;

- enable earlier identification of needs and earlier and more effective action to address these needs by providing a tool for practitioners to identify who else is involved with or has a concern about a child; and

- be an important tool to encourage better communication and closer working between different professionals and practitioners.

NB: Draft regulations were made to allow data matching trials to run between April and August 2006. The full detail of how it will operate, however, is not yet decided, so the following material is based on current government documents and the final regulations may be somewhat different. The DfES intends to publish draft full regulations for consultation this coming autumn.

The indexes will contain the following information on each child:

- basic details to identify a child and whether they are receiving universal services. These are name, address, date of birth, gender, a unique identifying number, name and contact details of a person with parental responsibility or care of the child, name and contact details for school or other educational setting, and names and contact details of GP practice and of any health visitor or equivalent;

- name and contact details for other practitioners involved with a child, so professionals can see who to contact if they wish to discuss a child's additional needs; and

- an indicator to show where a practitioner has important information to share, or is taking action in relation to a child, or where an assessment has been undertaken. It is in these terms that we will define "concern" (this indicator was originally called "a flag of concern").

At section 12(11), the Children Act 2004 specifically permits regulations for the database to be passed *"notwithstanding any rule of common law which prohibits or restricts the disclosure of information"*.

The index is not a substitute for the case record systems already being developed in health care (NHS Care Records – see Chapter 6) or social care (Integrated Children's System – see below). It will not hold data on children's needs, academic performance, attendance or clinical observations about a child. It will not contain the actual information these professionals hold, such as medical records. Additional numbers from existing case systems may be held by the Index in the background to improve accuracy or to allow a practitioner to find the Index record corresponding to his/her case record. The database will not record family relationships – but it will be possible to do searches listing all other children at the same address. Nor will the index indicate if the child is on the Child Protection Register since this is seen as sensitive case information. For children on the CP Register, the social worker can indicate on the index that he or she is involved

and wishes to be contacted in relation to that child, but the entry will not distinguish this type of concern from others.

The intent is simply for the database to facilitate contact between care professionals.

Processes for Data Entry

The database will be initially populated from the data held by the Department for Work and Pensions (they hold data on children because they pay Child Benefit to the carers of all children under 16, and some 16-19 year-olds). This data has good coverage; it has the right names, but tends to be bad on addresses. NHS databases have more current addresses, but less overall coverage. School (National Pupil Database) data is only just acquiring address data, but will also be included. The Office of National Statistics also has relevant records.

Thereafter, it is expected that as the care professionals who have access to the database create and update their own records, the information will be duplicated on the database.

In principle, data will be pushed on to the database from other systems and matched. Regulations will set out that users of the index shall take all such steps as are reasonably practicable to ensure that the information which the person or body has provided is and remains accurate and this includes notifying other data suppliers when information supplied is or appears to be inaccurate or incomplete. It will always be possible to say where data has come from. To deal with uncertainty, the system will display, for example, the address believed to be the most accurate, but other addresses supplied in connection with the child can also be called up to be viewed. If and when a definitive, verified address is ascertained, this will be stored and shown to enquirers. The results of the data matching exercise – and any corrections done to the automated process – will be retained to avoid repetition.

The database will be initially populated by feeds from a number of large-scale existing databases, e.g. the Department for Work and Pensions data on child benefit claims, the NHS database, and education. It will then be kept up to date by further updates from these and local systems such as Connexions and local social services systems. Data transfer will only be one way into the IS. There will be no feedback from the index back into individual databases. For example, if a GP records a change of address for a child, this will be automatically fed through to the IS. If a social worker then accesses the index information for that child, he or she will see the new address and can then update the social work records.

Access to the index would be granted according to the role of the practitioner. Detailed guidance on this will be included in the draft regulations to be published in the autumn. All practitioners and system support staff with access will have to have had relevant training and to have undergone appropriate checks, including Criminal Records Bureau checks and any additional checks introduced following the Bichard recommendations. Children and young people, and where appropriate their parents, will have the right to ask

to see their information and challenge it if it is wrong. The procedures for subject access will be included in the Statutory Guidance but are not yet available.

Since the system permits a view into 'factual' data held about the child by other agencies there does seem to be some potential difficulty with data accuracy. When a child moves to a new address, it will be obvious to anyone viewing the data which other agencies have not been told about the change. However, there does not seem to any provision for "pushing" information about this back to the originating agency. This seems a recipe for frustration at best and ongoing confusion between individuals at worst.

The data will be retained until the young person reaches 18. For some young people, who are in continuing need of a range of services (e.g. those with severe learning difficulties) it may be convenient to retain the records for longer. The young person's consent will be needed to do this but no entries will be kept past the age of 25.

Consent

Consent will not be required to record contact details for the majority of services. However, consent from children or their parents will be required to record contact details for targeted or specialist health services, where there is a strong public expectation and practitioner culture that information will only be shared where informed, explicit consent has been secured. The Government has decided that services related to sexual health, mental health and substance abuse should be the broad categories defined as sensitive. Where such consent has been given, the Index will only indicate that an unspecified sensitive service is working with the child. On-line access to further information will only be available to index management teams. Any practitioner wanting to contact the sensitive service would make a case to the index management team who would broker contact with the sensitive service practitioner. Children and parents will not themselves be able to specify which services they consider sensitive, and where they would like more privacy.

This appears to be quite contrary to data protection law and to the law of confidence as developed, for example, in Campbell v MGN Ltd. We will have much more to say about this in chapter 7. For now, we will merely remark that the Index as specified looks set to contain more sensitive data than Ministers appreciate, and that more attention to consent will be necessary.

Access

The following statutory services will have practitioners who will have access to the Children's Index: education, early years and childcare services, Connexions, health, social care, Youth Offending Teams, police, probation, prisons, YOIs and secure training centres. Local authority housing services and non-statutory voluntary services might also have practitioners with access, where appropriate. In many of these services, access will be through one or more central users (e.g. in a school, a SENCO rather than all teaching staff). All with access will have to have had relevant training and to have undergone appropriate checks.

Design of the Index

There will be a central index with the data partitioned into 150 districts, relating to each local authority in England. The justification offered for a central index is that it will ensure the system works for children who move areas, or who access services from more than one area. Each local authority will be a data controller with responsibility for maintaining the accuracy of the data.

Security

It is stated that clear and secure arrangements will be in place to guard against access by unauthorised users. The database will be accessed using two-factor authentication, and each access will be recorded against an individual user's name. All accesses will be audited in real time with systems that look for unusual patterns or levels of access. Audit logs will be kept for a few years, though not for decades. The index will be monitored for inappropriate use by authorised users, and there will also be regular, real-time scans for worrying patterns of behaviour, such as one user accessing a large number of records.

All children in England will be recorded. However the government considers that some groups of children will need a higher level of security to protect their personal data. Lord Adonis outlined that 'Children who have a reason for not being traced-for example, where there is a threat of domestic violence or where the child has a celebrity status-will be able to have their details concealed'[37]. The latest guidance states that there will be the facility for certain details to be blocked where a parent has good cause to believe that the inclusion of such information may lead to a crime being committed.

Cost

The estimated cost of this system is claimed to be £224 million over 3 years. Thereafter the annual ongoing operating costs are an estimated £41 million per annum. These costs are to ensure the accuracy of the data on the index, secure its operation, and train operators how to use it. The estimate also includes the operational costs of entering and accessing data by practitioners.

Nature of the Data

Much of the data is of a personal and factual nature but some may be very sensitive. The school attended may, for example, reveal the religion of the child or that he or she has a learning difficulty.

The indication on the index by a practitioner of involvement, having done an assessment, or having information to share (previously called a "flag of concern") is not clearly specified as yet but will be addressed in Statutory Guidance. It presumably will reflect a professional judgement about the child but the criteria for using this facility have not yet been formulated. When discussed by the House of Commons Select Committee as the

[37] Hansard, 20 March 2006, col.88

bill was going through Parliament, the Minister for Children failed to provide a clearer definition, although she was asked to. The level of concern at which practitioners enter an indication will be highly significant in determining the usefulness of the facility. A low level will flood the system with so many indications that they obscure more serious concerns.

Benefits of the Index: Child Protection

When the proposal for the Children's Index was first introduced to Parliament by Baroness Ashton, she linked it explicitly to its role in child protection, citing the recent murder of Victoria Climbié by her great aunt and the great aunt's partner after months of abuse and neglect:

> *"I believe that this system might have helped Victoria Climbié. It might have saved her life."* [38]

However, as already observed in Chapter 2, the problem in the Climbié case was not that the professionals were unaware of each other's involvement.

Lord Laming, who conducted the inquiry into the death of Victoria, was asked by the government to consider whether a national index would be a useful addition to service provision; the idea did not arise from consideration of the problems seen in the care provided for Victoria. The issue was discussed at one of the seminars that he held as part of his inquiry and his final recommendation was:

> *"The Government should actively explore the benefit to children of setting up and operating a national children's database on all children under the age of 16. A feasibility study should be a prelude to a pilot study to explore its usefulness in strengthening safeguards for children"* (Lamming, 2003, para.17.121.)

Eleven trailblazers had already been set up to develop methods for improving information sharing and nine of these opted for IT applications akin to an index. These were evaluated by a team from Royal Holloway, University of London, in the summer of 2004. The trailblazers have all operated under former legislation, since Section 12 of the Children Act 2004 (on the index) was only brought into force in January 2006. The evaluation did not produce detailed quantified data measuring the impact of the index on outcomes for children or professional activity, but reached general conclusions about the feasibility and desirability of an index.

The evaluation[39] identified that:

[38] Hansard, 24 May 2004, Col. 1160

[39] Department for Education and Skills, Learning from Information Sharing and Assessment Trailblazers. London, DfES

- *It had been established that outcomes for children would be improved if practitioners communicated and services were delivered in a co-ordinated way.*

- *An Index with details of how to contact other practitioners involved with a child could aid this process (para.20).*

Benefits of the Index: Safeguarding Children

The main benefit of the index is seen to be in facilitating the identification of, and effective response to, low-level problems in a child's health and development. As discussed in Chapter 2 above, it is believed that by offering effective help to low-level problems, fewer of them will escalate into serious, more intractable, difficulties.

Traditionally, practitioners have found out who else is in contact with a child by asking the child or parents. This avenue is still available to them, but it is thought that the index will be more efficient and time-saving.

There is no clear evidence that failure to provide services for low-level problems is due to failure to identify the problems. Many practitioners say that they fail to refer the child because the level of need does not meet the threshold for action of the service to which they would like to make a referral. Improving services for low-level problems therefore depends crucially on making adequate services available to meet the increased need – and this increase is considerable. The number of children estimated to have additional needs at any one time is 3-4 million. This is far higher than the number of children who develop serious problems.

The Every Child Matters programme is at such an early stage of development that it is not possible to judge its effectiveness yet.

3.3 Common Assessment Framework (CAF)

The purpose and rationale of the CAF is set out on the government's Every Child Matters website:[40]

> *The Common Assessment Framework (CAF) for Children and Young People is a key part of the strategy to shift the focus from dealing with the consequences of difficulties in children's lives to preventing things from going wrong in the first place. It is a nationally standardised approach to conducting an assessment of the needs of a child or young person and deciding how those needs should be met.*
>
> *The CAF will promote more effective, earlier identification of children's additional needs and improve multi-agency working. It is intended to provide a*

[40] Downloaded from www.everychildmatters.gov.uk, 21 February 2006.

simple, non-bureaucratic process for a holistic assessment of a child's needs, taking account of the individual, family and community.

The CAF has been developed for use by practitioners in all agencies so that they can communicate and work more effectively together. Information will follow the child and build up a picture over time. The CAF will encourage greater sharing of information between practitioners, where consent is given. It will:

- *Promote earlier intervention where additional needs are observed*
- *Reduce the number and duration of different assessment processes that children and young people need to undergo*
- *Improve the quality and consistency of referrals between agencies by making them more evidence-based*
- *Help embed a common language about the needs of children*
- *Enable information to follow the child*
- *Promote the appropriate sharing of information*

Children's trusts will be able to develop use of the CAF through non-statutory guidance.

The CAF is particularly suitable for use in universal services (health and education), to identify and tackle problems before they become serious. Using common assessment processes should streamline relationships between schools and specialist support services. Staff will need to be familiar with the CAF, which will support school's own ability to identify and deal with additional needs at an earlier stage. They will use the new database as an effective tool for making contact with other practitioners. Key staff, not all teachers, will form part of a wider team with other professionals to address individual children's complex needs.

If a common assessment suggests that a child has needs that require input from more than one service, it will help if one practitioner acts in the role of lead professional, to:

- *Provide a single point of contact, who children, young people and families can trust, and who is able to support them in making choices and in navigating their way through the system*
- *Ensure that children and families get appropriate interventions when needed, which are well planned, regularly reviewed and effectively delivered*
- *Reduce overlap and inconsistency from other practitioners*

The CAF will help practitioners undertake assessments in a more consistent way. In many cases, it will just formalise current practice. With the right attributes and/or training, we expect that practitioners in any agency will be capable of undertaking a common assessment. Where the assessment indicates that the child

has urgent or complex needs, requiring specialist assessment and intervention, the common assessment information will feed into the specialist assessment process.

Timetable for implementation

All local authority areas are expected to implement the CAF, as will be revised in early 2006, between April 2006 and the end of 2008. All areas should be working during 2005/06 to prepare for this, whether or not they implement the CAF published on 1 April 2005.

The CAF will be implemented during 2005/06 by local areas that choose to do so. This trial year will provide learning about the process of the CAF and associated checklist, in order to inform a revised version prior to April 2006. The DfES will commission a formal evaluation with a number of areas that are implementing the CAF and working to develop the role of the lead professional.

Range of Data Collected

The framework of the assessment echoes the established framework used in social work assessments of need and assessments of looked after children. Therefore it is already familiar to social workers, although it is a new venture for many other professional groups who have not been used to undertaking such holistic assessments. The practitioner completing the assessment is advised that they should consider each element but they do not need to comment on every one. They should concentrate on the presenting issues and explore areas around them to reach a more holistic view.
The data that may be covered includes:

- Basic details (name, address etc) of child or young person being assessed
- Basic details of all persons with parental responsibility
- Details of the person undertaking the assessment
- Name of lead professional (where applicable)
- Assessment data:
  - Date of assessment
  - What has led to the child being assessed?
  - Is the child disabled or are there any language or communication issues?
  - Details of agencies involved with the child

- The major sections of the CAF cover:

  1. Development of the child:

     health; emotional and social development; behavioural development; identity, including self-esteem, self-image, and social presentation; family and social relationships; self-care skills and independence; learning – including

understanding, reasoning and problem solving, participation in learning, education and employment progress, and achievement in learning, aspiration.

2. Parents and carers:

   Basic care; ensuring safety and protection; emotional warmth and stability; guidance, boundaries and stimulation.

3. Family and environmental:

   Family history, functioning and well-being; wider family; housing, employment, and financial considerations; social and community elements and resources, including education.

- Supporting evidence (strengths and needs identified) – to support the practitioner's conclusions and recommendations. The practitioner is advised to work with the child and/or parent or carer and take account of their views. They should record any major differences of opinion.
- Conclusions, solutions and actions
- Child's comment on the assessment and actions identified
- Parent or carer's comment on the assessment and actions identified.

The available documentation leaves a number of questions open. First, there are some technical security questions. For example, the eCAF Requirements Catalogue[41] reveals that in addition to access controls of the kind one might expect, the system will provide an access-control override for system-wide searches. If a user makes a search that includes material to which they do not have regular access, this will be audited; and if some item of data is so sensitive that it must be excluded from even audited system-wide searches, then it can be marked as 'shielded'. We doubt that the DfES appreciates the added complexity this introduces, from inference-security issues to the problems that have beset the 'sealed envelope' proposal in NHS systems. The Information Commissioner should keep a close eye on the evolution of this specification; as it stands it is unsatisfactory.

The proposed scope of the system also raises resource and compatibility issues. Will small services that do not at present have PCs be supplied with them, and what about GPs and hospital trusts whose computers are being ripped out and replaced with integrated systems supplied by Connecting for Health – will these systems provide an interface to CAF (assuming they can be made to work)? System interoperability, if achieved, would in turn raise further major privacy problems.

Consent for Recording and Sharing Information

The decision to carry out a CAF assessment is made by a practitioner. It is based on the practitioner's judgement that the child needs extra support to make progress towards the

[41] V 1.0, June 9th 2006

five priority outcomes the government has set out for children in ECM. The practitioner discusses with the family whether to proceed and does so only if they agree. The assessment is the practitioner's judgement about the strengths and needs of the child and family. There is a space for recording the views, wishes and intentions of the family and for recording differences of opinion but the dominant voice in the process is that of the practitioner.

The CAF form includes a section for the signed consent of the child and/or carer. If consent is given to sharing information, then the people or services with which the information may be shared are specified by the child or parent.

However, there are two consent issues that need further attention. The first is that, as the CAF is purely voluntary, abusive parents may always (and will in the medium term be likely to) withhold consent. This means that the CAF, and the ICS database which it feeds, cannot be held out as a panacea for abuse prevention; other mechanisms will be needed. And if CAF remains a system for the purely voluntary notification of low-level problems, then it is quite unclear what justification there might be for complex arguments about statutory gateways and other non-consensual means of data sharing.

Second, the issue of when information can be shared against the wishes of the child or parent illustrates many of the key concerns of this research report. What is the threshold at which a practitioner can and should allow his or her judgement of what is in the child's best interests to override the child or parent's judgement? The significance of this decision is often missed in government documentation by the habit of talking about the child's well-being as if it were an objective fact rather than a matter of judgement, thereby obscuring the fact that it is a subject on which people can and do rationally disagree. There is no one proven theory about the best way to raise a child, nor is there one clear pathway that children should follow to reach a healthy adulthood. At best, there are some useful theories about child rearing with some empirical support.

There is also a range of aspirations that people have for children. The government has stated its aspirations in the five outcomes it has specified in ECM. The five outcomes themselves are expressed in such broad terms that it would be hard to disagree with them but, at the level of the performance indicators, parents' aspirations for their own child may, at any one time, not coincide with the government's views. Nor may the parents' views of their child's progress towards those five outcomes coincide with the practitioner's assessment. This is an area where values, facts and theories are all significant in reaching a judgement on a child. The ECM agenda appears to be assuming that the government's and practitioners' views should be dominant, with the child and parents being overridden if they disagree. There are several significant child protection cases where courts have strongly disagreed with this view.

It is important to stress that the issue of parental abuse and neglect raises significantly different problems and this report is not criticising the well-established procedures for sharing information without consent in such cases. If the practitioner has reason to

suspect that the parent is abusive, then there are good grounds for overriding the parent's refusal to share information (or indeed not requesting consent in some circumstances).

3.4 Integrated Children's System (ICS)

The ICS will be an electronic case management system for workers in social care. It forms the core "electronic social care record" (ESCR) for children.

The DfES gives the following outline of how it fits with the ISA index and the CAF:[42]

> *It is hoped that, in the future, when a child is referred to children's social care and a referral is recorded on an electronic record system an electronic message will be sent to notify the IS Index of children's social services' involvement and to seek information about who else is involved. In addition, if a common assessment on the child exists, the information will easily be incorporated into the assessment sections of the Integrated Children's System because the information on needs in each system is organised on compatible lines. If a child needs to receive services from children's social services, the detailed assessment required for children in need will be given a head start with the information incorporated from the common assessment. This speeds things up, builds on existing knowledge and avoids the need for, often distressed, children or families to go over the same ground again.*
>
> *Other case record systems exist for children and young people, for example those held by Connexions or Youth Offending Teams. A similar relationship to that of the case records supporting the Integrated Children's System will exist between these case record systems and the ISA Index and the CAF.*

The ICS also has a part to play in improving the quality of assessment, decision-making, and intervention in social care.[43]

> *The lessons from research, inspections and inquiries into the deaths of abused children over many years have demonstrated the need for much more effective case record systems for children's social care. When children suffer neglect or abuse or need to be looked after, it is necessary to collect and record a great deal of detailed information about individual children. Furthermore this information needs to be gathered in such a way that it can be analysed for use in decision-making and presented in a number of ways for different purposes. Information, such as bedtime routines, favourite foods, allergies, etc., may have to be made available to a foster carer to help them look after a child introduced into their family. For the same child, information about his or her circumstances, family background, history, development etc., may have to be presented in a form acceptable to a court in legal proceedings to protect the child from harm. And yet*

[42] Downloaded from http://www.everychildmatters.gov.uk, 21 February 2006.
[43] Downloaded from http://www.everychildmatters.gov.uk, 21 February 2006.

again information about the child's progress will need to be presented to planning meetings and reviews and so forth. The Integrated Children's System is an applied conceptual framework for working with children in need and managing these detailed information requirements.

The ICS will include several forms, the key ones for children in need (including children in need of protection), in order of use, are:

- Contact record;
- Referral and Information Record (to be completed within 1 working day);
- Initial Assessment, including Initial Plan (within 7 working days);
- Core Assessment Record (within 35 working days);
- Child's Plan, which includes Child Protection Plan;
- Record of Strategy Discussion;
- Record of S47 Enquiries, which includes Initial Plan;
- Initial Child Protection Conference Report, which includes Outline Child Protection Plan;
- Chronology;
- Review Records;
- Closure Record.

For Looked After (i.e. 'in care') children, the following forms apply:

- Referral and Information Record;
- Chronology;
- Placement Information Record (which includes parental agreements and consents);
- Care Plan Parts 1 & 2;
- Adoption Plan;
- Pathway Plan Parts 1 & 2 (includes Needs Assessment);
- Review Record;
- Assessment and Progress Records;
- Closure Record.

It will be seen from these lists that the ICS will contain very detailed information about children and their families. It will include facts, opinions, and subjective judgements. The government's image of how the various services will co-operate to meet the needs identified by practitioners relies on sharing information freely between agencies. Therefore the issues raised by CAF on when practitioners will override the child or parents' wishes are pertinent to ICS.

There is also an issue about the extent of sharing information with or without consent. If one considers the sum total of personal information that might be written on these forms, when combined with the personal information on other forms in the wider system, there seems little space left for a private family life.

Chapter 4. School Systems

The children's agenda is not just about youth justice and social work, but about educational outcomes. In addition, the Department for Education and Skills (DfES) is the lead department for many of the cross-government initiatives we discuss. Therefore the existing school information systems are both relevant and important.

4.1 The National Pupil Database

Education is a devolved matter, so different systems operate in England, Wales, Scotland and Northern Ireland.

The National Pupil Database (NPD) records factual details of every child in state education in England. Wales operates a similar database, which interoperates with the English system (there is some extra information about the Welsh language in the Welsh database). There does not appear to be any similar central database in Scotland or Northern Ireland.

There is no requirement for the private school sector to provide data to the NPD although they have to provide statistical and summary information. In practice a few do work with the system but many do not.

Unlike many systems which are still at the planning stage, the NPD is a real, running, database, holding records at a national level. This data can be accessed by a small number of people within each Local Education Authority. Data about pupils in each school will be held by the individual schools. There are detailed standards for the data formats for transfer between these entities.

The legal basis for the NPD is set out in Chapter 7.

The Department for Education and Skills (DfES) is the data controller for the NPD. Individual schools will have their own data controllers.

The database is audited against BS7799. We were provided with the most recent review report on "PLASC (DSG: D1), Darlington" (November 2005) which showed that there were some relatively minor matters that needed to be dealt with, apparently delayed by a recent reorganisation, but that there no issues of major concern.

Database Fields

Initially, when it was set up in 2002 the NPD recorded the pupil's name(s), date of birth, gender, ethnicity, mother tongue and whether they were entitled to free school meals. To this was added data about the type of school they were attending, year group, when they

arrived, if they had been excluded, and what courses they were taking after the age of 16. The database also records the pupils' scores in the "key stage" tests usually taken at the ages of 7, 11 and 14.

In 2006 this has been extended to include the pupil's preferred surname and their address and postcode. The data on exclusions now indicates the reason and number of sessions missed. The database now records whether the pupil is "in care" or has a SEN (Statement of Special Educational Needs – i.e. they need extra provision to deal with one of a range of learning difficulties). There is also a flag for pupils who have been identified as "gifted and talented" (usually expected to be no more than 10% of the cohort).

The database fields are entirely matters of fact; there are no matters of opinion and no freeform text fields[44].

Some of the fields deserve further comment.

Database Field: Ethnicity

The ethnicity recorded in the NPD is recorded as two items; the ethnicity itself and the source of the information. The DfES guidance is that "In order to meet data protection requirements, it is essential that information provided by parents or pupils can be distinguished from information ascribed by the school".

However, it was not possible to identify any later processing that was paying attention to the presence of a qualifying field. For example, the National Statistical Office exclusion data[45] just uses the ethnicity data item.

Database Field: Free School Meals

Historically, entitlement to free school meals has been used as a quick and simple way of identifying deprivation. Hence it appears in the NPD as a way of processing data about schools within a social framework.

Database Field: The Unique Pupil Number

When pupils first enter an English school they are given a "unique pupil number". This is a structured value that consists of a code for the year, the LEA, the school and a number within that school that year. A check digit provides some integrity for the numbers when they are processed.

The practical purpose of the UPN is to permit data matching of information from the Qualifications and Curriculum Authority (QCA) and records of the same pupil from

[44] This may differ in the School Admissions system, whose database fields can be seen as a subset of those in the NPD. Although most fields in the admissions process are factual, some free-form subjective information, that has been provided by parents to support their choice of schools, can be transferred.
[45] http://www.dfes.gov.uk/rsgateway/DB/SFR/s000582/SFR23-2005.pdf

multiple schools. The DfES told us that it, in particular, it eliminated a lot of problems with assigning QCA results to the correct pupil record.

When the UPN was first being introduced, the Data Protection Registrar (as she was then called) came to an agreement with the DfES (then called the Department for Education and Employment) regarding the UPN. The main points of this agreement were that the UPN would lapse when pupils left school; the UPN would be a "blind number" and would only appear within computer systems; that it would be designated a "general identifier"; and that databases using UPNs would be encrypted and would have audit trails for authorised access.

A "general identifier" occurs in Schedule II of the Data Protection Act 1998. Paragraph 4 says:

> *"Personal data which contain a general identifier falling within a description prescribed by the Secretary of State by order are not to be treated as processed fairly and lawfully unless they are processed in compliance with any conditions so prescribed in relation to general identifiers of that description."*

In other words, it was intended that processing which used UPNs would be illegal except in tightly controlled circumstances. However, the UPN has never been so designated.

The DfES guidance to schools says:

> *"Schools should not enter UPNs on their admission register, or on pupils' paper files, and should continue to use the admission number, rather than the UPN, as a general pupil reference number within the school."* [46]

However, this guidance does not seem to be universally known and in one county we found that it was standard practice to mark pupil's 'blue folders' (the paper files on each pupil) with the UPN. It was seen as "obvious" that this was useful because the number would be needed when the blue folder was forwarded on to the next school that was attended. Although data would also flow electronically through the "s2s" (school to school) system, for ad hoc transfers (rather than mass movements from one part of the school system to another) the head teachers perceived the most important information flow to be telephone conversations with the head at the other school, followed by the arrival of the blue folder through the post.

UPNs are transmitted to other agencies along with educational data. For example, social services departments may be provided with the UPNs of children in care. However, the agreement with the Registrar has clearly limited their uses.

The UPN was only intended to be a content-free identifying number for data matching, and the structure within it is merely a convenience for issuing unique values. However, in practice this structure means that teachers are able to determine where pupils first entered

[46] http://www.teachernet.gov.uk/_doc/9083/UPN_Guidance_Update_2005_V1%20.doc

the state system, and at what age. The value of a UPN can also indicate that it was issued by an LEA – which would almost always mean a child was being assessed for special needs provision, a sensitive piece of information and perhaps not otherwise discernible. The Information Commissioner should consider issuing guidance on the extent to which identifiers that exist merely for data matching purposes should be permitted to contain this type of structure.

Although the numbers are said to be "unique", in practice they are not. The English and Welsh systems are entirely compatible, but some parts of the Scottish system also use UPNs, but – because their LEA identifiers overlap English values – the numbers may clash with those issued in England. Some schools in Northern Ireland, the Channel Islands and Gibraltar issue UPNs, but the DfES believe that at present there are no clashes in the values (although without control of these systems they cannot promise this will remain true).

When pupils change country (or move into the state sector from an independent school) UPNs may not be available. Schools are supposed to issue a temporary number and replace it with a permanent value when it is located. In some cases this leads to sufficient confusion that two UPNs are issued to the same child. There is a regular reconciliation process that should sort things out, but the NPD is designed to be able to record multiple UPN values so that data matching, particularly of prior attainment levels, will continue to be possible.

However, sometimes UPNs get assigned to the wrong child, and the DfES has had to issue detailed guidance on how to avoid this being recorded in the NPD as a duplicate UPN – with the consequent risk of further confusion between the children.

The DfES are planning a "Unique Learner Number" for use within the QCA for tracking those involved in "lifelong learning". The indications are that, unlike the UPN, this will be a public number.

Transfer of Data Into the NPD

These days, data about pupils is often held on computer within school information management systems rather than on paper files. Besides basic data about pupils there may be photographs, contact phone numbers for carers, details about timetabling and much other useful information.

Use of a computer is mandatory for some information because specific data items must be passed to the Local Education Authority (LEA) via an annual process called the Pupil Level Annual School Census (PLASC), which occurs in mid-January.

PLASC is in the process of being replaced by a new process called the School Census. This subsumes other data collections such as "Forvus" that took place in other times of the year. The School Census will occur three times a year (in September, January, and May) though there are minor differences in the data items transferred on each occasion.

The DfES argue that "The vast majority of the data will be that which a well-prepared school would already be holding and keeping up-to-date for its own purposes".[47]

Taking part in PLASC (and now the School Census) is a statutory requirement. The first regulations to be issued[48] in 1999 allowed pilots of PLASC to be carried out. These were revoked in 2000 by Regulations that extended PLASC to all state-maintained schools,[49] which were in turn revoked in 2001 by regulations that increased the range of information collected.[50] A series of amendments – but not revocations – to the 2001 regulations have followed, the most recent (2005)[51] requiring more than 40 separate data items, including information about school attendance, and the full postal address of pupils.

Transfers of Data From the NPD

The DfES publish a document on "fair processing"[52] which lists the bodies to which pupil data may be transferred by a school. These include the LEA and the DfES (meaning in practice the NPD). Other bodies are the Qualifications and Curriculum Agency (QCA), Ofsted (the school inspectors), the Learning and Skills Council and also Connexions service providers. The DfES document gives the text of an example notice to be sent to parents. The notice appears comprehensive and includes details such as which databases the child may be on and who to contact to make subject access requests.

Transfer of Data to the Qualifications and Curriculum Authority

The QCA uses data from the NPD to administer the testing and assessment for key stages 1 to 3. The results from the tests are then passed back into NPD. Ensuring that these flows of data operate correctly is the main purpose for the Unique Pupil Number (see above).

Transfer of Data to Connexions

There is a legal requirement in Section 114(1) of the Learning and Skills Act 2000 to pass information on request to the Connexions service for pupils in or approaching the Connexions age range (essentially secondary age pupils). Connexions is intended to "encourage, enable or assist (directly or indirectly) effective participation by young persons in education or training". However, s117(2) permits a person over 16, or his parents if the person is under 16, to forbid the supply of any information other than the name and address of a pupil and his parents. In other words, there is an 'opt out' for further information such as ethnicity, examination results, SEN status or exclusion information.

---

[47] http://www.teachernet.gov.uk/management/ims/datacollections/scbackground/
[48] 1999/989 The Education (Information about Individual Pupils) (England) Regulations 1999
[49] 2000/3370 Education (Information About Individual Pupils) (England) Regulations 2000
[50] 2001/4020 Education (Information About Individual Pupils) (England) Regulations 2001
[51] 2005/3101 The Education (Information About Individual Pupils) (England) (Amendment) Regulations 2005
[52] http://www.teachernet.gov.uk/_doc/9146/FPN%20guidance%202005.doc

Sometimes information passes from the school, but sometimes via the LEA, which is why the opt-out information has to be passed via PLASC and stored in the NPD. The legal basis for this is found in Regulations.[53]

The DfES advice[54] is that to give parents or pupils who wish to opt out an adequate opportunity to do so, information should not be passed to Connexions until four weeks after the notice is sent to them. Parents or pupils are entitled to register an opt-out subsequently, even if they do not do so within the initial four-week period. In that event, no further information should be passed to Connexions after the opt-out has been received.

The DfES advice goes on to say that Connexions partnerships "will not generally pass on any information which they receive about pupils without discussing this with them first". The Connexions Code of Practice for Professional Advisers[55] sets out the exemptions as being where child protection issues are involved; where there is a significant threat to life; where the young person needs urgent medical treatment; and/or where potential or actual serious criminal offences are involved.

It should be noted that there is also a "Connexions Card" available to all between the ages of 16 and 19. This is a smartcard which permits the collection of points for learning, work-based training and voluntary activities. There are also discount schemes associated with it, and it can act as a proof-of-age card.

DfES and Capita, who jointly manage the Card, deal with the fair processing issues for pupils approaching or above age 16 as they become eligible for a Card. Schools taking up the Connexions Card are required to sign an agreement containing explicit undertakings that they will inform pupils that personal details are being passed to the Connexions Card Team, and give them the chance to tell the school if they do not wish this to happen.

4.2 Ofsted Systems

NPD data is passed to Ofsted who feed it into systems called PAT (Pupil Achievement Tracker) and PANDA (Performance and Assessment Reports). These are being replaced by a single product called RAISEonline (Reporting and Analysis for Improvement through School self-Evaluation).

Fundamentally, these schemes take performance data for individuals and schools and compare it with other individuals and schools. The analysis is presented in the form of graphs for cohorts and individuals permitting the identification of strengths and weaknesses of schools and individuals. For example, it can show that a school is failing

[53] 2002/3112 Education (Information About Individual Pupils) (England) (Amendment) Regulations 2002
[54] http://www.teachernet.gov.uk/_doc/9146/FPN%20guidance%202005.doc
[55] http://www.connexionswestyorkshire.co.uk/dbfiles/955347319/pacodeof.doc

to ensure that mid-range ability pupils progress as well (relatively) as those at the extremes of the ability range.

The data in these reports are used by Ofsted for their school inspections, and by schools for self-assessment. In particular, schools use it for target-setting for individual pupils, and tracking progress towards those targets throughout the school year.

We were told that although many schools benefit from these systems, they were fairly naïve in their projections, just drawing straight lines from previous results. Go-ahead schools were using their own target-setting systems that divided a cohort into smaller groups and applying different factors to each group. Teachers still needed to adjust the targets for individual students and individual subjects, but the initial estimates were much more realistic than the generic government-supplied systems.

The targets are typically given to the pupils as a minimum level of achievement and an aspirational level. If progress was unsatisfactory, then the school would intervene with extra tuition or other help. The idea as explained to us is "to turn D's into C's and possible C's into definite C's". Besides improving the life chances of the pupils, this would ensure that the school would come out well when inspected.

We discussed these systems with a teacher at a large (1400 pupil) comprehensive that catered for 14-18 year olds. We were told that although their intake was almost entirely from four middle schools, there were wide variations in ability from year to year and the school had to adjust their teaching accordingly. However, the LEA refused – citing Data Protection – to pass the school any data on pupils, until the admissions process was complete in July. This left them little time to see what needed to be done. The school ideally wanted the data in January instead (though in some areas this will not include key stage 2 results). Of course there would be no Data Protection issues if they were given anonymised data about the cohort (which would be just as valuable since 98% or so of the pupils would arrive anyway). This appears to be just another case of a body citing 'Data Protection' as an excuse not to do something rather than considering what data the school actually wanted – which was just a statistical overview of the particular year group.

The same teacher also drew our attention to the work of the Fisher Family Trust in this area of the prediction of attainment. They use the pupil's postcode to split the cohort into groups based on social background. This improves the estimates considerably at later key stages. As ever, data items – such as postcodes – have rather more significance than might at first appear.

4.3 Lost Pupils

When pupils leave a school they must be taken "off roll" (so that their places will not be funded by the LEA). Their data will be transferred to the new school using the s2s system (as noted above). In most cases the school or LEA will know what the new school will be (especially when transferring between primary/middle/secondary schools).

Alternatively the new school will make contact, seeking the data that can then be transferred, as noted above. When this does not occur the pupils are placed into a "lost pupil database".

What is supposed to then happen is that a newly arrived pupil, perhaps returning from a trip abroad or from the independent sector, will be located by name, date-of-birth etc, within the lost pupil database by the LEA (not by the school, which is not permitted to search the database in this way). This will reveal their UPN and their previous school, which can then be contacted.

In practice, pupils seem to stay in the "lost pupil database" although they appear within PLASC returns from their new schools. In September 2005 the DfES reported[56] that there were 4400 "lost" pupils of whom about 50% appeared on PLASC 2003 returns.

The DfES offer guidance on dealing with situations where it is intended that the previous school is not told where the pupil has moved to – for example when the family is fleeing a violent partner. The LEA should ensure that the data is moved electronically using a special destination code so that the new school location is not divulged. However, this scheme does depend upon the school being told of the family situation and this information being passed to the LEA operative who actually does the transfer. It might reasonably be argued that where "lost pupils" were involved there was no reason to tell the old school what the new one was in any circumstance, which would fix the specific problem by employing a general data protection regime.

4.4 School Admissions

The data about pupils is also used for the school admissions process. Parents indicate their preferences for the school that their child will attend. Where necessary the applications will be forwarded, often as electronic datafiles, to another LEA or to a school that is its own admissions authority. The LEAs or schools then offer places on the basis of this information. The datafile records contain a subset of the information as in the PLASC process such as names, addresses, "in care", and are augmented by details of siblings, reasons for wishing to apply for particular schools etc.

Because schools are permitted to select on matters such as faith, these records can contain sensitive information. There is also provision for a "SocMed" reason for requesting admission to a particular school. It indicates that there is further social/medical information about the pupil being sent under separate cover.

The regulations for schools clearly indicate which matters can be taken into account when making their admission decisions. However, this appears to be driven by a wider political agenda as to how schools are to be permitted to determine who they admit, rather than being based on a data protection approach. It is reasonably clear that the envisaged mechanism is that sensitive information, such as that relating to faith, will only

[56] http://www.teachernet.gov.uk/management/ims/datatransfers/s2s/forlea/

be transferred to schools that can make use of it, but there does not appear to be any explicit guidance to that effect.

4.5 Cross-Government Guidance on Sharing Information on Children and Young People

The Department for Education and Skills (DfES) has recently consulted[57] on a guidance document on sharing information about children and young people. The guidance will be non-statutory, but it is intended that it will be endorsed by the DfES, Department of Health, Home Office, Office of the Deputy Prime Minister and the Department of Constitutional Affairs.

We talked with the officials who are dealing with this consultation. They told us that their aim was to make practitioners "confident and competent" when dealing with questions of data sharing although at present "people find this area hard".

The first stage of their model applies only if the person with the data works for a statutory body. They must identify a "power" to share the information. If no such power exists then the action is likely to be "ultra vires" and the sharing should not occur. The suggestion is that the question to be asked is "do I need to share information to do my job effectively?" in which case an implied power is likely to exist. They then identify statutes such as Section 2 of the Local Government Act 2000, which provide wide-ranging powers that are likely to be applicable.

The consultation notes that few "powers" make it compulsory to share information. Conversely only in a few areas – such as attendance at sexual disease clinics – is it unlawful, per se, to share information.

The second stage of the Government model is to apply a legal test to the particular disclosure. They identify the need to conform to the Data Protection Act 1998 and the common law duty of confidence. It is also observed that the Human Rights Act 1998 must also be complied with – although it is very likely that meeting the DPA and common-law requirements will ensure conformance.

The document sets out a number of principles for data sharing, with the overriding one being the safety and welfare of the child or young person. It stresses that consent to sharing should be obtained "unless it is not safe or possible to do so". The document also covers the need to record decisions and to ensure that data is accurate, held securely and kept no longer than necessary.

The consultation document is significant in that it shows at least part of government accepts the difference between a "vires" and a statutory gateway. However, there are a number of lacunae.

[57] http://www.dfes.gov.uk/consultations/conResults.cfm?consultationId=1366

One of the illustrative examples (of a non-communicate child attending a playgroup) is particularly objectionable. It suggests that the playgroup leader should seek consent to share her concerns with health practitioners – and she should indicate in any letter she wrote “that her concerns would increase if this is refused”. Such statements raise very serious issues which we shall consider in detail in Chapter 7 regarding informed consent, Gillick Competence, coercive consent and the manner in which consent is sought.

Chapter 5. Tackling Youth Offending

The duty on local authorities to prevent youth offending, set out in the Crime and Disorder Act 1998, has led to a growing emphasis on risk assessment and pre-emptive services that seek to 'divert' children before they offend. The concept of identifying and tracking children who possess characteristics that might predispose them towards committing criminal offences in the future first came to public attention in 2001, when Sir Ian Blair (then Deputy Commissioner of the Metropolitan Police Service) referred to it in a speech to the Youth Justice Board.[58]

At the time, the suggestion caused considerable concern and there was no further public airing of government or police plans to introduce any such scheme. However, over the past few years a number of initiatives, assessment tools and related databases have been rolled out to identify children who have not committed any offences, but are thought to be more likely than average to offend in the future, and to profile young offenders in order to predict and prevent re-offending.

The most significant of these tools are the ASSET and ONSET profiles, and the RYOGENS database. ASSET is used with young people who have already come into contact with the criminal justice system, while ONSET is used to identify children thought to be "at risk" of offending. Both were developed for the Youth Justice Board of England and Wales (YJB) by Oxford University's Centre for Criminological Research.

The information gathered using these tools is shared within multi-agency Youth Offending Teams (YOTs) and Youth Inclusion and Support Panels (YISPs). RYOGENS initially focused on the identification of children of any age who were thought to show early signs of becoming offenders, but it is now being developed to share more general concerns about children across a range of agencies: social services, housing services, police, education, health, Connexions and YOTs.

5.1 ASSET and ONSET

ASSET was introduced in 2000 across the youth justice system in England and Wales. It is a portfolio of structured assessment tools designed to build up a profile of each young offender by examining the contributory factors that may have brought a young person into contact with the criminal justice system. The ASSET profile is held on the YOTs information management system – either the Youth Offending Information System (YOIS) from Social Software, or the Careworks system – and can be shared electronically. It is used to prepare reports that will inform court assessments and

[58] 'Naughty children to be registered as potential criminals' http://news.telegraph.co.uk/news/main.jhtml?xml=/news/2001/11/25/ncrime25.xml&sSheet=/news/2001/11/25/ixhomef.html

interventions.[59] Detailed information is recorded by members of a Youth Offending Team in a 24-page Core Profile about education, family circumstances, living arrangements, lifestyle, substance abuse, physical and mental health, attitudes to offending, and motivation to change.[60] Various additional tools are available to assess issues such as drug use, risk of harm and vulnerability.

The assessments are scored in each category for adverse factors, and the score is then used to predict the likelihood of re-offending. An evaluation carried out by Oxford University's Centre for Criminological Research in August 2005 (the designers of ASSET) found that ASSET scores could predict reconviction within 2 years with 69.4% accuracy.[61] However, the meaning of this statistic is unclear since the base rate and the rates of false positives and false negatives are not reported. We have not been able to find any independent evaluation of the ASSET system, although we cannot categorically state that none exists. Evaluation is in any case problematic unless randomised controlled trials are conducted, because of the many factors that have a bearing on re-offending.

The eAsset sentence management system is the YJB's proposed system for juvenile offenders in the secure estate (i.e. any institution in which a child or young person is detained as a result of a criminal charge or conviction). It gives staff the ability to use ASSET profiles prepared before sentence as the basis for sentence planning decisions, and makes them into active documents that can be exchanged and updated by staff both in the community and the secure estate. The system has been piloted since 2004 in Wetherby and Lancaster Farms Young Offender Institutions (YOIs) and is due to be extended to all 21 YOIs during 2006.[62]

It should be noted that some practitioners express concerns in respect of the use of subjective opinion rather than facts in building up ASSET profiles, and also about the lack of independent evaluation of the ASSET system referred to above.

The related ONSET assessment tool is intended to help identify young people considered at risk of offending.[63] It is being piloted with 13 Youth Information and Support Panels and "identifies the needs, risks and protective factors associated with the child or young person's involvement in offending and anti-social behaviour".[64]

---

[59] Youth Justice Board of England and Wales. Asset – Young Offender Assessment Profile. Available from http://www.youth-justice-board.gov.uk/PractitionersPortal/Assessment/Asset.htm

[60] Youth Justice Board of England and Wales. ASSET Core Profile form. Available from http://www.youth-justice-board.gov.uk/NR/rdonlyres/4912382F-9286-4695-8CE3-9B33C0D26249/0/3CoreProfile.pdf

[61] Further Development of Asset. K Baker, S Jones, S Merrington and C Roberts, Youth Justice Board for England and Wales 2005. Available from http://www.youth-justice-board.gov.uk/Publications/Downloads/Asset%20full%20report%20fv.pdf

[62] Graham Technology. Case study: Youth Justice Board. Available from http://www.grahamtechnology.com/Home/IndustrySolutions/Government/CaseStudies.jsp

[63] Youth Justice Board of England and Wales. ONSET Assessment. Available from http://www.youth-justice-board.gov.uk/PractitionersPortal/Assessment/ONSET.htm

[64] Youth Justice Board of England and Wales. Quality Standards for Youth Inclusion and Support Panels. Available from http://www.youth-justice-board.gov.uk/NR/rdonlyres/B93020FE-06F0-49FF-AB12-EF72265A1047/0/QualityStandardsforYouthInclusionandSupportPanels.doc

The six-page ONSET assessment form gathers information on contact with police and social services, family circumstances, educational history, lifestyle, substance abuse, physical and mental health, attitudes to offending and motivation to change.[65] If an ONSET assessment of a child suggests the presence of at least four risk factors, YISP Management Guidance suggests that he or she be referred to the YISP.[66]

ONSET profiles can be shared electronically using software such as the Youth Justice Board's YISPMIS (YISP Management Information Service),[67] whose user interface can be seen below.

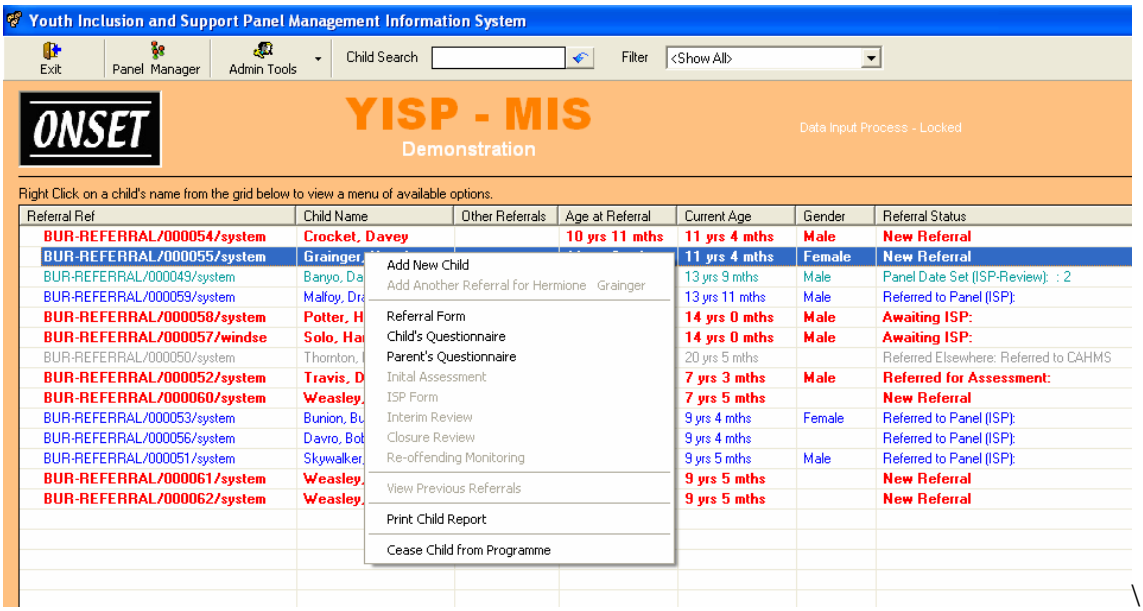


Figure 5.1

5.2 Reducing Youth Offending Generic National Solution (RYOGENS)

RYOGENS was funded in May 2003 by the Office of the Deputy Prime Minister (ODPM) as part of the e-Government National Projects programme, and developed in partnership with Warwickshire County Council, Tower Hamlets and Lewisham. It has since received further ODPM and local authority funding, and now has three additional

[65] Youth Justice Board of England and Wales. ONSET Assessment. Available from http://www.youth-justice-board.gov.uk/NR/rdonlyres/1B36963A-E539-4690-8714-EC6A73B6C97C/0/FullAssessmentVersion2May2005.doc

[66] YISP Quality Standards p. 12

[67] Youth Justice Board for England and Wales. YISPMIS User Manual, May 2005. Available from http://www.youth-justice-board.gov.uk/NR/rdonlyres/DB5EE50E-FBEF-4634-9B75-359F8A3D71B5/0/YISPMISUserManual.doc

partners: West Berkshire, Redcar & Cleveland and Coventry. Lewisham is no longer a partner.

In December 2005 the project migrated from the ODPM to Esprit Ltd, the system's software developer, and is now called "ShareCare: RYOGENS". The focus is on broadening the scope of RYOGENS beyond prediction of youth offending, as Esprit explains:

> *"We are developing the RYOGENS technical solution to be a generic tool to assist the identification, assessment, referral and tracking over time of vulnerable children and young people."* [68]

RYOGENS is a centrally-managed database that is accessed by practitioners in the partner local authorities via the Internet. It allows workers in social services, education, health and youth justice teams to share details of minor concerns they hold about children, based upon factors derived from ONSET and the Department of Health's Framework for the Assessment of Children in Need and their Families.

When practitioners are adding a concern about a young person to RYOGENS, they are asked to provide further evidence for that concern. A list of possible concerns is provided below. Some of these lend themselves to simple factual evidence, such as "missed medical appointment" or "living in high-crime area"; others are more open to interpretation: "lack of family support" and "parental lack of awareness of child's needs", for example. The concerns are based on ONSET and a similar Department of Health framework which both give emphasis to factors that are believed to be associated with the onset of offending.[69]

ONSET-related Concerns Within RYOGENS[70]

- Victim of bullying/harassment
- Perpetrator of bullying/harassment
- Negative home influence on education
- Poor school attendance/truanting
- Bad behaviour in school
- Exclusion from School
- Learning difficulties
- Substance availability
- Child: substance misuse
- Parent: substance misuse
- Animal Cruelty
- Has intent to harm others

[68] RYOGENS Frequently Asked Questions p. 3. Available from http://www.localegovnp.org.uk/default.asp?sID=1107356827748
[69] RYOGENS FAQ, supra, pp.19-22
[70] RYOGENS FAQ, supra, p.10

- Dangerous behaviour
- Denies involvement in anti-social behaviour/crime
- Suffering actual harm
- Has harmed others
- Self-harm
- Involvement in anti-social behaviour/crime
- Social Isolation
- Non-constructive spare time/easily bored
- Parent: mental health
- Parent: physical health
- Not registered with healthcare professional
- Missed medical appointment
- Child: sexual health
- Child: physical health
- Child: mental health
- Child: mental well-being
- Living in high-crime area
- Family and/or peers involved in anti-social behaviour/crime
- Domestic conflict/violence
- Caring for relatives at home
- Financial and/or housing difficulties
- Parental lack of awareness of child's needs
- Absent from home
- Lack of family support
- Frequently moving house
- Lack of facilities/equipment
- Parenting difficulties
- Other

The DoH Framework is almost identical.

As one practitioner says: "RYOGENS allows you to flag up much 'softer' concerns at a stage earlier than identifying significant risks".[71]

The part of the system that allows these concerns to be entered into the system is shown below in Figure 5.2.

When the number of concerns held within system reaches a user-configured limit between 1 and 40 (all of the pilot schemes have set this to 1), an alert is generated for the local authority's RYOGENS Management Function, responsible for making a preliminary assessment and ensuring that alerts are followed up promptly and appropriately through a referral to a specific service when required.

[71] R Hill, S Jones, C Roberts, K Baker. Probation Studies Unit, University of Oxford. An Evaluation of the early application and piloting of RYOGENS, May 2004 p. 29

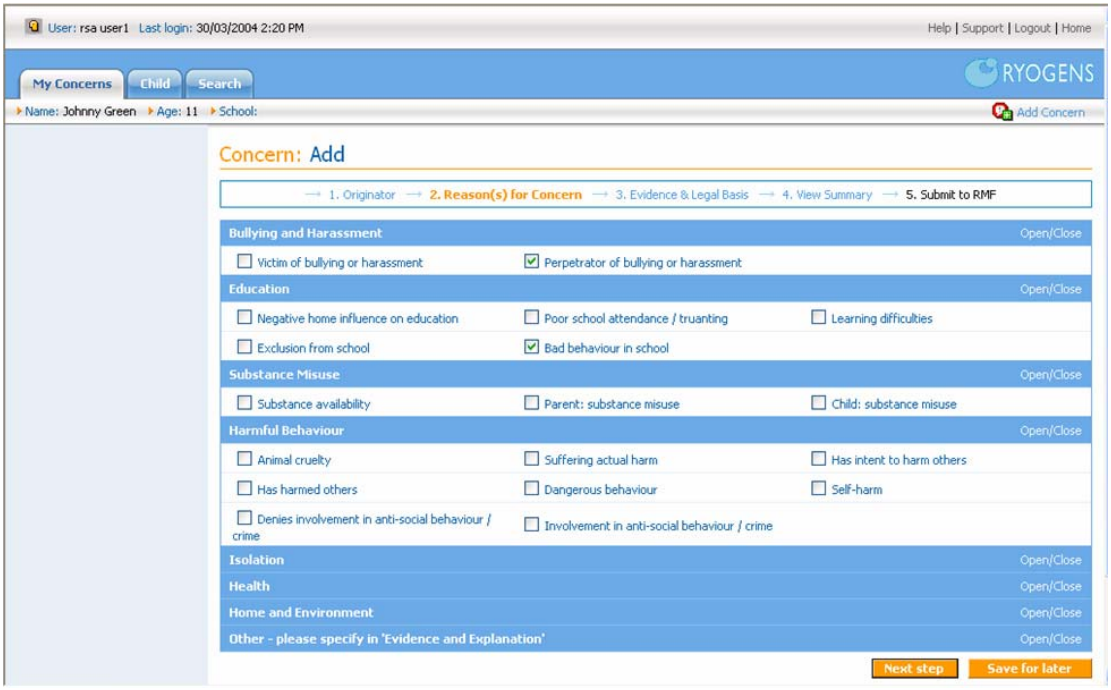


Figure 5.2

Consent

Both ASSET and ONSET emphasise that young people must give their consent before data collected about them is shared. ASSET's Effect Practice document states: "It is important that consent is obtained from the young person and their parents/carers for the collection of the information".[72] ONSET's Guidance Notes state that: "A referral will not usually be accepted at the YISP without valid and completed consent".[73]

However, RYOGENS takes a different approach, providing a list of legislative bases for information sharing without consent that practitioners can select from a drop-down menu if a young person or their carers will not consent to the sharing of personal information. This list was reviewed by the Department for Constitutional Affairs, by the three initial pilot local authorities' legal departments and by Caldicott guardians.

[72] Youth Justice Board for England and Wales. Key Elements of Effective Practice – Assessment, Planning Interventions and Supervision p.8. Available from http://www.youth-justice-board.gov.uk/Publications/Scripts/fileDownload.asp?file=AssessPlanning.pdf

[73] Youth Justice Board for England and Wales. ONSET guidance notes, May 2005 p. 6. Available from http://www.youth-justice-board.gov.uk/NR/rdonlyres/01D0B466-71C4-4410-80D6-9330D751857A/0/GuidanceNotesV2May2005.doc

Legal Basis for Sharing Information Within RYOGENS Without Consent[74]

- Safeguarding/promoting the welfare of children who are in need.

  Children's Act 1989, Section 17 (1): duty of every LA to safeguard and promote the welfare of children who are in need. Need includes those who are "unlikely to achieve or maintain a reasonable standard of health or development".

- Taking reasonable steps to identify children in need.

  Children's Act 1989, part 1 of schedule 2, paragraph 1. Applies to LAs and professionals in other sectors.

- Preventing children from suffering ill-treatment or neglect.

  Children's Act 1989, part 1 of schedule 2, paragraph 4. Applies to LAs and professionals in other sectors.

- Promoting social inclusion (including the reduction of risk factors).

  Section 2 of the Local Government Act 2000 – discretionary power for LAs to do anything likely to promote or improve the "economic, social or environmental well-being" of their area. The aim is to help LAs ensure service delivery is co-ordinated in ways that minimise duplication, maximise effectiveness and present a concerted approach to the causes of complex problems such as social exclusion.

- Improving the physical and mental health of the population.

  National Health Service Act 1977 – only applies to health functions and other agencies carrying out health service functions.

- Ensuring that primary/secondary education is available to meet needs.

  Education Act 1996

- Encouraging participation in education or training.

  Learning and Skills Act 2000 section 114: authorises providers LA, PCT, Police, Probation, YOT, LSC providing services to 13–20 year olds to share information with Connexions and imposes a duty of confidentiality.

[74] RYOGENS FAQ, supra, p.12

- Preventing or reducing crime/crime and disorder.

  Crime and Disorder Act 1998 applies to LA, Police, Probation and Health.
  Section 115 – authorises disclosure of information where it is necessary or expedient for the prevention and reduction of crime.
  Section 117 – do all that it can to prevent crime and disorder.

- In accordance with local Information Sharing Agreement and statutory duties

The first evaluation of RYOGENS in Warwickshire, Tower Hamlets and Lewisham found that this ability to over-ride the requirement for consent was widely used. Of the alerts generated by RYOGENS (when a concern had been noted), consent had only been obtained in 20% of cases. Lewisham obtained 46% of cases:[75]

> *[T]he majority of practitioners are relying on legislative exemptions to justify noting a concern, for example, one police officer noting a concern about a nine month old baby on the grounds of preventing crime and disorder – the aim of this provision was to protect against the individual, in this case a 9 month old baby, so appears to have been used incorrectly. This situation obviously should not continue and more consideration needs to be given to the subject as a whole. Does there need to be more detailed guidance on the web-site for example?*
>
> *Should there be more emphasis given to the practical application of consent during training on the system? Do practitioners (especially those not traditionally dealing in the area of risk and need e.g. GPs, nurses, teaching assistants, community group leaders) need guidance on how to approach parents/carers and young people about the possibility of concerns being logged on to the RYOGENS system? Is the relevant literature for parents/carers or young people reaching its intended audience? What processes are in place for the RMF to deal with the misuse of legislation?*

The RYOGENS software has since been re-designed to respond to these and other concerns expressed in the evaluation. Practitioners are now encouraged to obtain consent before sharing information, only using legislative exemptions to this requirement as a last resort. Some local authorities, such as Redcar & Cleveland, require staff to obtain a sign-off from a line manager before using this capability. Others, such as West Berkshire, are recording contact details of practitioners who have had contact with a young person rather than storing details of concerns, allowing other practitioners who encounter that young person to make contact directly and then negotiate the sharing of any information.

Local authorities are responsible for producing their own guidance to parents and young people on the information they wish to gather and what data subjects' rights are. Some pilot local authorities sent out this guidance in mailshots to parents.

[75] RYOGENS FAQ, supra, p.42

The initial RYOGENS evaluation was clear that the minimal use of legislative over-rides of consent is critical for confidence in the system from all parties: "Evidence from the 'On Track' [dealt with elsewhere in this chapter] evaluation shows that practitioners (and young people) need to be absolutely confident that the information put on to the system is treated responsibly and is only acted upon where deemed appropriate".[76]

Regulatory Aspects

Local authorities participating in RYOGENS are the data controllers. They process and share personal data under their corporate entries in the Data Protection Register. The developers of RYOGENS work with each new local authority user to document their information sharing protocol, and build that into the controls on data sharing in RYOGENS. Lewisham's scheme is documented at the RYOGENS website.[77]

The RYOGENS Management Function within each local authority can grant access to specific cases to team members, with read-only and write access. In the latest version of the software, consent can be withheld for sharing with specific teams, people or services, but users can over-ride this by providing a reason (which is added to the audit trail); many local authorities require that an administrator or lead practitioner also gives consent for this to occur.

The RYOGENS developers state:

> *"We have not attempted significant integration to existing systems, nor to develop sophisticated case management. The intention is that RYOGENS will be a quick and new interim solution to current needs."* [78]

Local authorities are able to configure the access levels of each of their RYOGENS users. This can include restricting access to data to the relevant department. However, because modern practice is to have multi-agency teams working across departments, the existing pilot schemes have only restricted access to RYOGENS users within the authority.

Sources and Recipients of Data

RYOGENS is implemented by local authorities in conjunction with the voluntary sector. It is populated by practitioners within those agencies with concerns about local children, and can be further restricted by geography and age range.[79] While later versions of the system will automatically link with the Department for Education and Skills' Information

[76] RYOGENS FAQ, supra, p.51
[77] Document available from http://www.localegovnp.org.uk/webfiles/National%20Projects/Ryogens/Toolkit/Deliverables/EXAMPLE%20A%20Guide%20to%20Lewisham's%20ISP_v001_160304.doc
[78] RYOGENS FAQ, supra, p.4
[79] RYOGENS Local Vision and Scope Statements

Sharing (IS) system and ONSET,[80] it does not provide comprehensive coverage of young people within a local authority.

The developers say: "we see RYOGENS as a building block or stepping stone to meeting the challenges posed by IRT".[81] (Identification Referral and Tracking, or IRT, was the previous term for what is now referred to as ISA – see chapter 3 above.) The next version of the software (due March 2006) will include support for Common Assessment Framework data.

Consolidated reports can be produced by RYOGENS to assist local authorities with the management of their services, but these reports do not contain personal data.

Data Quality, Staff Training, Fitness for Purpose

Interviews with RYOGENS users in the initial evaluation found that practitioners were aware that the lack of a rigid format for the evidence required could be problematic. One stated: "everybody who's cautious about [information sharing] is right to be… you need to be in regards to sharing personal and sensitive information, and often subjective and possibly wrong information."[82] Another noted: "Very little consistency as to the concerns noted in each of the pilot areas and in the number of concerns entered at one time."[83]

Another problem was that some less-qualified practitioners saw the system as a way of recording a large number of concerns and leaving their more qualified colleagues to make decisions on the significance of that information. A community warden in Lewisham commented: "I don't want to have the responsibility of making a decision when I'm entering concerns. I'm not a qualified social worker so I would rather enter all the information and let the experts decide which is the best avenue open".[84] Automated profiling occurs, but only to the extent of generating alerts when the number of concerns registered about a young person exceeds the number configured by the RYOGENS Management Function.

As for data retention, each local authority sets its own retention policies. Different services have different statutory requirements, and can have access for different periods of times once a young person is no longer covered by RYOGENS. Data subjects can be automatically excluded from searches once they reach the age of 18, but system administrators need to take specific action to permanently delete data.

Security Procedures and Technology Used

The developers of RYOGENS see its design as a centrally-managed system as a means by which security can be carefully controlled. It uses a four-tier architecture, with clients

[80] Department for Education and Skills Information Sharing and Assessment Update – Issue 4, 29 July 2004 p. 1
[81] RYOGENS FAQ, supra, p.4
[82] RYOGENS FAQ, supra, p.33
[83] RYOGENS FAQ, supra, p.47
[84] RYOGENS FAQ, supra, p.31

connecting using Web browsers to a Web server that is separated by a firewall from an application server that is connected through another firewall to the database server. [Ryogens FAQ p.6]

The developers of RYOGENS have undertaken Criminal Records Bureau level 2 checks on staff with access to the system, and encouraged local authority pilots to do the same.

Independent penetration testing has been undertaken three times on RYOGENS without any successful access to information in the database (although on one occasion, false data was inserted into the database.)

An audit trail of all data accesses and modifications is kept.

5.3 National Register of Unaccompanied Children

The National Register of Unaccompanied Children (NRUC) is a system being developed by the Association of London Government to exchange information between the Immigration and Nationality Directorate (IND) of the Home Office and local authorities that are caring for unaccompanied under-18 asylum seekers. It was launched on 23 November 2004 by Des Browne MP, the Home Office Immigration minister.[85] Unaccompanied children from overseas are also being considered for inclusion in the database.

NRUC's primary aims are to ensure that local authorities receive timely and appropriate funding for providing this care, and that these children are kept track of as they move between boroughs.[86] Its key objectives are to provide accurate and timely information to statutory agencies, stop adult asylum seekers claiming to be children who are entitled to stay in the UK until their 18th birthday,[87] and facilitate performance management.[88]

NRUC is an Internet-based system designed to automate existing processes that rely on the physical transfer of spreadsheets between the Home Office and local authorities via floppy disks sent through the post. Data is transferred via an interface with the IND's A-CID database, and will be updated by local authorities. This data will contain all of the information needed for local authorities to make a grant claim and to ascertain the status and details of children in their care.[89] An audit trail is kept of all changes made to the database.

[85] http://www.dfes.gov.uk/ISA/learnFrmLocalAuth/relatedProject.cfm
[86] What is the NRUC? http://www.nruc.gov.uk/nruc.html
[87] Under the Immigration Act 2001, the Home Office is responsible for adult asylum seekers but local authorities are responsible for children, reimbursed by the Home Office.
[88] What are the objectives of NRUC? http://www.nruc.gov.uk/objectives.html
[89] How it Works. http://www.nruc.gov.uk/howitworks.html

The user interface is shown in Figure 5.3.

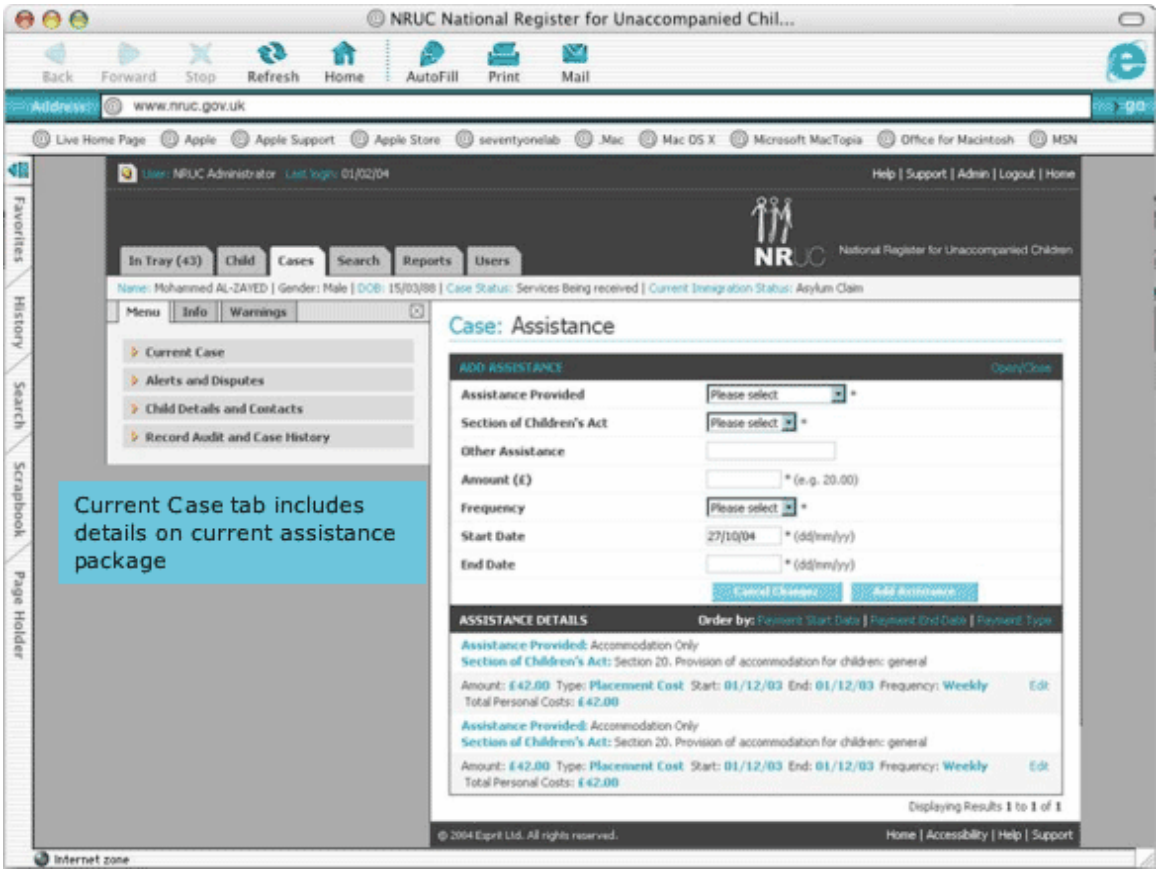


Figure 5.3

Participating authorities and agencies so far include:

- Westminster City Council
- London Asylum Seekers Consortium
- Association of Directors of Social Services
- Association of London Government
- Local Government Association
- Home Office:
  - Immigration and Nationality Directorate
  - National Asylum Support Service
  - Integrated Casework Directorate
- Department of Health
- Department for Education and Skills[90]

[90] The NRUC Partnership. http://www.nruc.gov.uk/partnership.html

NRUC is also working with the following NGOs:[91]

- National Society for the Prevention of Cruelty to Children
- United Nations High Commissioner for Refugees
- International Red Cross
- ECHO – EU Humanitarian Aid Office
- Save the Children UK

The NRUC database is open to monitoring by agreed organisations promoting children's and refugee's rights. Currently, only the Refugee Council has this status, with limited read-only access. This access will be extended to other NGOs, but the methodology for doing this is still under discussion in the project's steering group. Anonymised reports can be produced for NGOs.

Necessity of Consent in Sharing Data

Local authorities have individual policies on the consent that is required from individuals before sharing different categories of data processed by NRUC.

Regulatory Aspects

Information is shared between local authorities and the Home Office under provisions of the relevant immigration acts. These bodies are the data controllers. The Home Office's data protection registration number is Z7271689.

A steering group which includes childcare professionals guides the development of NRUC. The group has not produced any specific guidance on privacy and security issues. The Association of London Government and ESPRIT, the system developers, have together defined the security policy for the system.

Categories of Data Shared and Controls on Sharing

The name, date of birth, country of origin and Home Office case number are the only mandatory data items stored. Other data can be stored to facilitate tracking of individuals and case handling. This is mainly related to assessments that local authorities have made of the assistance needed by each child, details of placements, and other costs incurred that should be reimbursed.

Data is owned by the local authority where the child resides, and cannot be viewed by other authorities. A limited subset of this information is shared with the Home Office to facilitate reimbursement of care provided. Within authorities, access to service-specific data can be restricted to relevant departments. However, post-Climbié, most authorities allow teams to access the whole range of stored personal data. Staff must undergo Criminal Records Bureau checks before being given database access. When a local

[91] Links. http://www.nruc.gov.uk/links.html

authority comes into contact with a child who has previously received care from another local authority, the system provides contact details with the relevant case worker so that any necessary information can be manually exchanged.

It is planned that NRUC will link to IRT (now ISA, or IS) systems, and other linked data resources, to allow the tracking of unaccompanied children using a single system.[92]

The identities of children that have been rescued from people traffickers are extremely sensitive. The Refugee Council has commented that these children's identities must be "defended from those who see them as assets not individuals."

Data Quality, Staff Training, Fitness for Purpose

The personal data stored is largely objective. It certainly achieves its primary objective of ensuring that local authorities are reimbursed by the Home Office, sometimes slowly, for the care that they provide to unaccompanied children!

Does Automated Profiling Occur?

No. The data supplied to the Home Office using NRUC (which previously was supplied using a laborious spreadsheet mechanism) may be used to identify newly-adult asylum seekers that are no longer eligible to remain in the UK.

How Long is Data Retained?

Data is archived, as under the Children (Leaving Care) Act 2000 provisions (s.20) and their interpretation in the *Hillingdon* case local authorities in some circumstances must provide care until young adults reach the age of 24. After this point the data is deleted.

Security Procedures/Technology Used

NRUC is designed as a three-tier system accessed via the Internet with protection for the database and the software querying it. All registered users are assigned permissions to access and modify specific data in the system.

5.4 Notify

NOTIFY is a web-based notification and information system whose stated design goal was to improve homeless households' access to services. Its primary role is to notify relevant services of the placement or movement of homeless households placed in temporary accommodation by London boroughs under homelessness legislation. It will also produce comprehensive information on homelessness and temporary accommodation in London. The system uses information provided by London borough housing

[92] Asylum seekers: Lone children to be placed on register *Young People Now* 6 October 2004. Available from http://www.ypnmagazine.com/news/index.cfm?fuseaction=full_news&ID=5153

departments to notify housing, education, social care, and health services about homeless households placed in, moving between or leaving temporary accommodation.[93] Its principal funding came from the ODPM, the London boroughs and the GLA.

The following information on Notify can be found in its nomination for an award by the New Statesman: [94]

- *There are currently over 64,000 homeless households (of which around 70% contain children and 15% are placed outside their 'home' borough*

- *Each week, every borough in London uploads to NOTIFY a range of details about each of its homeless households in temporary accommodation, in a simple report format. The system then compares the current week's information with the previous week's. Where it identifies that a household has moved into or out of an address, NOTIFY creates a 'notification' to the relevant department or agency. Authorised users log on to the NOTIFY notifications website and see a targeted summary of the notifications relevant to their organisation, displayed in priority order (eg health users see lists divided according to whether or not households contain pregnant members or children under 5, education users see only those households containing members aged 19 or under). Users can then access more detailed screens about each household. Information that is not relevant or allowed to be shared with a particular user is not displayed, so for example housing departments are not able to see any details about social services involvement with a household. All authorised users receive a weekly email that summarises the number of notifications they need to view on the system.*

The NOTIFY FAQ provides more information: [95]

- *There is a detailed NOTIFY Data Sharing and Security Agreement and also the system has been designed so that information is available for viewing on a strictly need to know basis.*
- *London borough housing departments, social services departments and local education authorities plus London primary care trusts [participate]. These agencies participate because they provide key statutory services.*
- *Security surrounding the system and information about the system was, and still is, a priority during all aspects of the development, implementation, and running of the system. Security of NOTIFY, relating both to hardware and software, conforms to advice provided by leading experts in the field. All users must be registered and go through a*

[93] See http://www.notifylondon.gov.uk/
[94] See http://www.newstatesman.co.uk/nma/nma2004/nominate2004.php3?Action=Specific&URN=http://www.notifylondon.gov.uk
[95] See http://www.notifylondon.gov.uk/doc.asp?doc=29&CAT=23

stringent process of verification before being granted access to notifications website.

- *Once a week data is uploaded onto NOTIFY and an email is sent to the registered users in housing, social services, education and health. This tells them how many homeless households have recently moved into, within and out of their borough. They can then access the notifications website and find out more about these households.*
- *NOTIFY covers households placed in temporary accommodation by London borough housing departments. While most temporary accommodation being used by London boroughs is located within Greater London, there are several hundred households being accommodated outside the Capital. Where households (being dealt with by London boroughs) are placed in, move between or leave temporary accommodation outside London, notifications will be made to agencies in the relevant local authorities.*
- *A NOTIFY Advisory Group was set up in February 2002, to support and assist the NOTIFY Project Team. This brought together practitioners from relevant fields – housing, health, education and social services – as well as IT and information management specialists and officers involved in other e-government initiatives. In addition, there were detailed discussions with key stakeholders over the course of the project development, including a series of workshops and multi-agency meetings in the local authorities that participated in the original NOTIFY pilot.*
- *In London, the vast majority of households applying as homeless are placed in temporary accommodation, often for long periods of time. This is because of the shortage of permanent council and housing association homes.*
- *There are certainly other groups of homeless people living in temporary accommodation, such as asylum seekers being supported by social services departments or the National Asylum Support Service (NASS). Like those accommodated under the homelessness legislation, they often have particular difficulties accessing services. Because it is a new and groundbreaking system, that has cost a lot of time and money to develop, in the first instance it has concentrated on one particular group of homeless people. However, it has been designed to be flexible and it will be possible in the future to add additional groups of homeless people and additional organisations to the system.*

It was expected that the advisory group would convene on a quarterly basis, with its first meeting taking place in July 2005.[96] We have not had time to contact the group between learning of it and completing this project, and have not been able to find minutes online.

Under the Housing Act 1996, local housing authorities are required to notify each other when a homeless household is placed in temporary accommodation within the boundary

[96] See http://www.notifylondon.gov.uk/doc.asp?doc=56&CAT=74

of another local authority. In addition, the Code of Guidance accompanying the homelessness legislation states that where households have to be temporarily accommodated in the district of another housing authority, the placing housing authority should take positive steps to ensure effective liaison and co-operation between the relevant service departments of both authorities, including housing, social services, environmental health and education.[97]

At NOTIFY's press launch in June 2004, it was claimed that the system would give local services constant access to information about homeless people moving in and out of their area, so they will be able to ensure that babies are immunised, children have school places and vulnerable children don't slip through the net. ODPM homelessness minister Yvette Cooper said NOTIFY would play an important part in ensuring that people in temporary accommodation don't lose out on essential services just because they have been moved across borough boundaries. She said: [98]

> *"It is important that local authorities in London know someone's support needs as soon as possible, and that these services are in place ready for when that support is required."*

When the system was being planned, in 2002, it was reported that [99]

> *"Apart from questions of privacy and security – we're talking about data that might identify people as child abusers – there is the technical problem of interoperability… The only reason the authority's scheme has any hope of working is something called the e-government interoperability framework (e-GIF). This is a set of standards being drawn up as part of the Office of the e-Envoy's e-government programme. It will require all government systems to be able not just to transmit data to each other, but to understand each other's data in context."*

So far, so apparently reasonable. However, once the system had been launched, the Climbié case cited to spur on those councils who had been late in supplying information to the system. The Guardian reported in October 2005: [100]

> *"Local authorities were warned today that they are risking another Victoria Climbié tragedy because housing departments are failing to provide information on where homeless families are living across London. Councils in the capital were told by the Greater London Authority (GLA) last year to provide weekly updates on where they had placed homeless people for Notify, a cross-capital database that tells social service departments about the vulnerable people who*

[97] http://www.nexusdesign.com/about_us/press_releases/24-10-2002.htm
[98] LH magazine: Joining up to help homeless, S Stevenson, at http://www.londonhousing.gov.uk/doc.asp?doc=12794&cat=1660
[99] http://technology.guardian.co.uk/online/story/0,3605,839264,00.html
[100] `Councils 'risk another Climbié tragedy', A Ricketts, Guardian, Oct 21 2005, at http://www.guardian.co.uk/child/story/0,,1597873,00.html

have moved into their area. But almost 18 months into the project almost half of London councils have still not submitted any data, leaving huge holes in the information, Inside Housing reported today."

This must be a classic case of deliberate confusion between child protection and child welfare, with child-protection concerns being misrepresented to justify child-welfare systems. A lawyer would point out that although a homeless child is a "child in need" under section 17 of the Children Act 1989, that still does not give local authorities a power to share information without consent. It is only in a situation where a child is "at risk" (section 47), or where the Housing Act 1996 applies, that they can do that.

5.5 Preventive and Low-level Systems

The picture that emerges of the myriad schemes and local systems for monitoring and targeting children thought to be at risk of becoming offenders, or who are engaged in low-level crime, is one of considerable confusion. The time available to prepare this report limits the extent to which these systems can be examined in the depth that is undoubtedly required, but it seems clear that there is widespread information-sharing, for which consent is considered a matter of good practice rather than law. In many cases the extent of information sharing is governed by locally agreed information-sharing protocols. However, it is not always clear whether the limits on who can access sensitive information, and in what circumstances, are well defined.

The Youth Justice Board has issued guidance on sharing information about children thought to be at risk of offending,[101] which sets out as follows:

By following this guidance, it should be clear that agencies are able to share personal data, even without the consent of the data subject, across a range of existing and planned partnership arrangements. These partnerships include:

Youth Offending Teams (Yots)
Safer School Partnerships
Children's Fund Partnerships
Child Protection Teams
Youth Inclusion and Support Programmes (YISPs)
Information sharing and assessment.

However, this document will be relevant to any partnerships that aim, principally or otherwise, to prevent crime by children and young people through the provision of early support and intervention to reduce identified risks.

[101] Sharing Information on Children and Young People at Risk of Offending: A Practical Guide www.youth-justice-board.gov.uk/Publications/Scripts/fileDownload.asp?file=infosharing0305.pdf

Exchanging personal and sensitive personal information between agencies, without the consent of the data subject, is seen as difficult and this is often used as an excuse for not doing it. However, in the context of preventing or reducing crime and disorder, and given the legislative framework within which the agencies referred to in this guidance operate, such exchange of information can, in fact, normally be done lawfully.

...

Although a Youth Offending Team (Yot) is not in itself a legal entity, it is a statutory partnership of named local agencies, which are all listed above: as such, this guidance applies equally to data-sharing within and by a Yot. Through a variety of common law, prerogative powers, and legislative provisions, all of these bodies have the required lawful basis for disclosing personal information for the purpose of preventing or detecting offending by children and young people.

...

Even where there is a prima facie lawful basis for information-sharing, it may be that some of the information held by the relevant bodies is such as to come under the common law duty of confidence... Where there is no statutory duty to disclose, because of the context and purpose of the proposed information-sharing it is considered that an overriding public interest in disclosure is likely to arise such that disclosure can still be made. It is therefore considered that the law of confidence should rarely prevent disclosures in the current context.

Consent, although desirable, is not essential for agencies to share personal information in the circumstances envisaged in this guidance... However, obtaining consent remains a matter of good practice, as opposed to a requirement of law, where the purpose of sharing information is not prejudiced by notifying the data subject at that time. In practice, because of the voluntary nature of preventive support and intervention, the direct involvement of the data subject will be necessary at some stage. Any need to share personal information without consent is, therefore, expected to be minimal and is likely to be restricted to the early identification stage of those children and young people who are at risk.

It should be remembered that "at risk" refers to the possibility that the child or young person may become an offender in the future, having been identified by a practitioner as exhibiting certain characteristics, or living in a particular environment.

Youth Inclusion Programmes (YIPs) operate in high-crime areas, targeting the "top 50" children aged 13–16 identified as being most at risk of social exclusion, or likely to truant or commit offences.

Junior YIPs operate along similar lines to YIPs. They aim to reduce social exclusion, offending and "other adverse outcomes" by targeting 8 to 12-year-olds said to be at "high risk".

Information is held on the Youth Inclusion Programme Management Information System (YIPMIS). Children are identified for YIPs through the YJBs "ID50" process on the following criteria:

Yot
Young people are considered to be at risk if they have been referred to or contacted by the Yot and if at least one of the following applies to the young person:

- *previously convicted*
- *previous custodial sentence*
- *received Yot disposal or equivalent pre-Yot.*

Social services
They are also considered to be at risk if they have been referred to or contacted by social services and if at least one of the following applies:

- *accommodated by voluntary agreement with parents (s20 CA 1989)*
- *subject to a care order (s31 CA 1989)*
- *remand to local authority accommodation (s23(1) CYPA 1969)*
- *his/her name has been placed on the child protection register*
- *any other referrals to or contact with social services*
- *any social services involvement with siblings.*

Pupil Referral Unit
Young people are seen as being at risk if they have been referred to or contacted by the Pupil Referral Unit of the LEA and at least one of the following applies:

- *permanently excluded in the past 12 months*
- *received a fixed-term exclusion in the past 12 months*
- *truanting at least two-to-three days per month in the past 12 months*
- *other referral.*

Police
They are also considered at risk if they have been referred to or contacted by the police and at least one of the following applies to the young person has:

- *been arrested in the past 12 months*
- *been convicted in the past 12 months*
- *had other contact such as persistent juvenile nuisance/anti-social; or behaviour order in the past 12 months*

School
Young people are considered as being at risk if they have been:

- *permanently excluded from school in the past 12 months*
- *received a fixed-term school exclusion in the past 12 months*
- *truanting at least two-to-three days per month in the past 12 months*

Connexions
The young person has been referred to or contacted by Connexions. Specifically, at least one of the following applies to the young person:

- *permanently excluded in the past 12 months;*
- *received a fixed term exclusion in the past 12 months*
- *truanting at least 2 to 3 days per month in the past 12 months.*

Junior YIP
The young person has been referred to or contacted by the Junior YIP. Specifically, at least one of the following applies to the young person:

- *currently/previously in Junior YIP core 50*
- *previously referred to the Junior YIP*
- *involved with a negative peer group*
- *siblings or other family members involved in offending.*

Positive Futures
The young person has been referred to or contacted by Positive Futures. Specifically, at least one of the following applies to the young person:

- *currently/previously in Positive Futures core group*
- *previously referred to Positive Futures*
- *known to be offending but not in the youth justice system; or*
- *siblings or other family members involved in offending.*

Youth Inclusion and Support Panel
The young person has been referred to or contacted by the Youth Inclusion and Support Panel (YISP). Specifically, at least one of the following applies to the young person:

- *referred to the YISP*
- *known to be offending, but not in the youth justice system;*
- *given acceptable behaviour contract*
- *siblings or other family members involved in offending.*

Youth Service
The young person has been referred to or contacted by the Youth Service. Specifically, at least one of the following applies to the young person:

- *known to be offending but not in the youth justice system*
- *involved with a negative peer group*
- *involved with drugs*
- *siblings or other family members involved in offending.*

Other
Young people are also seen as being at risk if they:

- *have been causing a nuisance in the YIP area*
- *are known to be offending but not in the youth justice system*
- *are involved with a negative peer group*
- *have siblings or other family members involved in offending.*

Under the heading "How to complete the ID form for 'other'" the ID50 guidance says:

> *"The Youth Inclusion Programme realises that there are a number of young people living in YIP areas that are not known by the local statutory agencies. However, these young people are nonetheless presenting concerns. It may be that young people are not enrolled at a school, are offending but not getting caught, or are causing a nuisance on the estate. Whatever the reasons, there are clearly young people that are at risk but are not known by local agencies: the YIP must endeavour to access these young people. We believe that there is a considerable amount of local intelligence with regard to these young people – the YIP should assume the role of an identifying agency by collating information about these young people from local contacts, residents, tenancy associations, community groups, street wardens, etc. This information should be used to complete the ID form for 'other'. However, in co-ordinating this part of the process, YIPs must remember that non-professional sources of information may be considerably more subjective than any professional body – this must be considered when identifying the 50."* [102]

The ID50 guidance also advises that information can be shared at local and national level on the basis of: "The data protection act 1998, the Youth Justice Board's information sharing protocol and section 115 of the Crime and Disorder Act". Disaggregated information can be shared within the YOT and YIP; however, only case numbers are attached to information that goes beyond these partnerships.

[102] ID50 Guidance for Partners http://www.youth-justice-board.gov.uk/NR/rdonlyres/0233E9E7-8E58-45E0-ACF8-E3190B8EAD19/0/ID50guidancedocumentforpartners.doc

An evaluation of YIPs conducted in 2003 concluded that:

> *"In terms of meeting the programme's outcomes, however, the evidence is mixed. On one hand there are early signs of success. There is evidence that the majority of the top 50 are being arrested less since their engagement on the programme, and for less serious offences. In addition, there has been a reduction in exclusion from schools (albeit the data on this issue is far from comprehensive). On the other hand, there is inescapable evidence that the programme appears to be falling short of the current target that three quarters of projects will have experienced a 30% reduction in crime by March 2004. Despite some encouraging reductions in crime in selected project areas, this overall finding is disappointing."* [103]

Mention has already been made above of the use of the ONSET tool in YISPs. The Youth Justice Board believes that this could also be extended to YIPs and Junior YIPs.

Positive Futures is a Home Office initiative developed in partnership with Sport England and the Youth Justice Board by the Home Office's Drug Strategy Directorate, which describes it as:

> *"a sport and activity-based early intervention programme that aims to have a positive influence on participants' substance misuse, physical activity and offending behaviour."* [104]

The programme is aimed at marginalised young people from 10–19 years of age, and priority is given to engaging those young people living in deprived neighbourhoods. From April 1st 2006, management of Positive Futures will be passed to 'Crime Concern'.

'On Track' targets 4 to 12-year-olds and their families in twenty-four high crime, high deprivation areas in England and Wales. It was established by the Home Office in 1999, and subsequently incorporated into the work of local Children's Funds.

Positive Activities for Young People (PAYP) provides "diversionary activities" targeted at 8-19-year-olds who are identified and referred by YOTs, Connexions, Behaviour Improvement Programme (BIP) schools and other agencies as being at risk of social exclusion and community crime.

'Prolific and Other Priority Offenders' (PPO): Prevent and Deter

The title of this Home Office strategy is somewhat misleading: it has three strands, and the first of these (Prevent and Deter) is aimed at young people who are not prolific offenders. They are either thought to be potential offenders, or they are involved in low-level crime.

[103] Evaluation of the Youth Inclusion programme, Morgan Harris Burrows, July 2003
[104] http://press.homeoffice.gov.uk/press-releases/positive-futures-future-decided

However, supplementary government guidance acknowledges that:

> *"We recognise that this cannot be an exact science. We cannot be certain that a particular young offender will become a PPO without additional intervention, or that a young person will certainly turn to crime."* [105]

The scheme operates through local Crime and Disorder Reduction Partnerships (CDRPs), and data is held on the local PPO Performance Management System. In practice, much of the work may be carried out under existing schemes already outlined above; guidance issued by the Home Office, DfES and YJB[106] advises that:

> *Work to develop the prevent and deter model locally should build on existing children and young people-focused provision. This may include early prevention programmes (such as Sure Start), those targeting at risk children and young people (such as Youth Inclusion Programmes, Positive Futures) and work with young offenders or those at risk of harm from substance misuse*
> …
> *YOTs may well provide the focal point for much of this activity. But Children's Trusts, Children's Fund partnerships and the local providers of services for children and young people represented on both YOTs and CDRPs (which include education, health, social care, criminal justice, social inclusion, leisure, youth provision and family support) will need to work together to ensure that, in the local area, there are community-based interventions and support programmes for both the most at risk young people and the most active young offenders.*

Antisocial Behaviour: a variety of systems exist at local level, operated by CDRPs or local Antisocial Behaviour Units, to collect and share information about allegations of antisocial behaviour, and details of those issued with Antisocial Behaviour Orders (ASBOs) or Acceptable Behaviour Contracts (ABCs). ABCs are issued to those under 18, or to parents if a child is aged under10. They have no legal status and any representations are heard by the local authority that issues them, including evidence from 'professional witnesses'. ABCs are generally described as 'voluntary' agreements; however the sanctions for breaching them can include eviction and applications for ASBOs or Parenting Orders.

Police Systems

It appears that a similarly confusing situation exists with regard to police systems. In some areas, child protection information is held separately from intelligence about children coming to the notice of police for other reasons. Other areas place all such information on the same system. As we have already observed, it is not possible to study

[105] Prolific and other priority offender scheme: supplementary guidance relating to the prevent and deter strand August 2005 http://www.gos.gov.uk/gol/docs/247610/london_model.doc
[106] Prolific and other priority offender strategy guidance paper, Prevent and Deter, September 2004 http://www.crimereduction.gov.uk/ppo02_guidance.doc

the full extent of information systems and data-sharing within the constraints of this report, but we are able to give some examples.

The 'Nipper' Database operated by North Yorkshire Police and the Safer York Partnership holds details of truancy, missing children, those who may be at risk of harm, and of children whose behaviour is deemed unacceptable for reasons ranging from alcohol abuse to "inconsiderate activity whilst playing games – for example ball games in the street".[107] When a child is entered on to the system, an automatic notification is generated to the police ward manager and to the City of York council.

MERLIN is a system operated by the Metropolitan Police to record every instance of a child 'Coming to Notice' (CTN). This is also known as a 'Form 78', after the manual CTN system that pre-dates the MERLIN database. The instructions to officers give the following non-exhaustive list of reasons for entering a child on the database:

- Evidence of Prostitution
- Runaway
- Subject of Prosecution – A child or young person who has been arrested and is either:
    - Informed that the police are not proceeding with the case despite having sufficient evidence to prosecute
    - Released on bail pending further investigation
    - Issued with a penalty notice for disorder
    - Informed of no further action because of insufficient evidence to prosecute
- Truanting
- Victim of Crime
- Arrested – This includes when a child is present when parent/s or carers are arrested
- Breach of Child Curfew
- Bullying
- Child Care/Welfare: When a pregnant woman comes to police notice, the MERLIN CTN must be completed in circumstances where the welfare of the unborn child gives cause for concern.
- A child who is on the child protection register
- Child Found Wandering
- Child found to be suffering or experiencing mental health problems
- Families where Mental Health issues are known or suspected, whether in an adult (where children are in the household) or child
- Domestic Violence incidents where a child or children are present at the time whether in the same room or elsewhere in the house
- Domestic Violence Incidents where children are part of the family but not in the location at the time of the incident

[107] http://www.saferyork.org.uk/pdf/2004_06_nipper.pdf

- A child who is the subject of a care/wardship order has been found in circumstances giving rise to concern.
- A child who is present when police are searching premises
- Any other kind of activity whatsoever, that might increase the likelihood of a child becoming involved in offending or where the child or family may, in the officers' judgement, benefit from the intervention of local social services.
- Child U/10yrs Criminal Act – any action on the part of a child under 10 that would justify an application for a child safety order under Section 11 of the CDA (e.g. where the child has committed an act which would amount to an offence if he/she were over 10).
- Intra-Family Abuse – a child has been found in circumstances of potential harm giving cause for concern, for example where it is identified that a child lives at the home and the family members are involved in a domestic violence incident and/or they are dependent or there is suspicion of substance abuse.

The MERLIN system is accessible to all Metropolitan Police officers and civilian staff (once they have completed training to use it) and police in any London borough can check the entries for other boroughs. In almost all circumstances, a MERLIN notification will be faxed to the local social services department. If education or health services have signed up to an information-sharing agreement with the Metropolitan Police Services, they may also receive MERLIN information.

5.6 Young Offender Systems

Although the systems for dealing with children after conviction for a criminal offence are not a prime focus of this report, there are some important issues that merit discussion. We describe some of these below, and provide an outline of some of the systems that have come to our attention.

A number of information systems (and assessment procedures) relate specifically to young offenders. Concerns expressed by practitioners include the very high level of information sharing, the lack of any clear exit strategy from certain specific lists, and the destination of files containing highly sensitive information that accompany young offenders.

Youth Offending Teams have their own case-management systems (YOIS, referred to earlier) and submit quarterly statistical returns to the Youth Justice Board (YJB) via the THEMIS system.

Sentencing: details of any sentence received by a young offender will go to the Home Office, the YOT for the area where the child normally lives and the YJB. Custody placements of juveniles are tracked on the YJB SACHS database (Secure Accommodation Clearing House System).

Schedule 1: If the offence falls into the categories set out in Schedule 1 of the Children and Young Persons Act 1933, the young person may be placed on to a local authority register of 'those presenting danger to children'. This registration is for life, and details will be forwarded to other local authorities as the child moves.

There is mounting concern about the disproportionate implications for young offenders of this policy, and the whole system is currently under review by the Government. In particular, the Safeguarding Vulnerable Groups Bill currently before Parliament provides for significant changes to current procedures.

Dangerousness: If an offence is one 'specified' in schedule 15 of the Criminal Justice Act 2003, then the young person must be assessed for "dangerousness" (where the court is of the opinion that there is a significant risk to the public of serious harm). NACRO is concerned that:

> *"The ASSET Risk of Serious Harm assessment was not designed for the purposes of determining dangerousness in relation to the new sentencing powers. In the first place, while serious harm within the context of the new provisions is defined as meaning 'death or serious personal injury, whether physical or psychological', there is no equivalent definition in the Youth Justice Board guidance on completing the relevant section of ASSET. Practitioners may therefore be working to a lower standard of risk in conducting such assessments than that required by the legislation."* [108]

The implications are serious, because custody – an "extended sentence", possibly indefinite – is the inevitable outcome of being deemed dangerous, and there are also implications for post-release.

Yellow Envelope: After a child receives a custodial sentence, the custody escorts are handed the 'yellow envelope'. This contains important information about the child for the receiving institution. The system was introduced (and welcomed) because vital information was sometimes lost, or was not delivered urgently enough.

Some practitioners have raised concerns about the destination of the yellow envelope after the child has gone through reception procedures. Sometimes the envelope seems to be held in discipline, or through-care, but it is not clear that there is an established protocol for safeguarding what is highly sensitive material. This issue might be followed up with the YJB.

Post-Release

On release the child will be on the police **NOMIS** (National Offender Management) system, and the local YOT system. S/he may also come under the 'Rehabilitate and Resettle' strand of the Home Office PPO system described earlier, in which case an entry will be held on the Crime and Disorder Reduction Partnership system.

[108] NACRO Youth Crime Briefing June 2005: Dangerousness and the Criminal Justice Act 2003

MAPPA and VISOR: If the offence involved "dangerousness", s/he will be referred to MAPPA (Multi Agency Public Protection Arrangements) and will also automatically go on to the new police VISOR (Violent and Sexual Offenders Register). Practitioners express concern that there do not appear to be clear exit strategies for young people from these systems. This is an important issue because the behaviour of children and young people, and the danger they present to others, can change radically as they mature.

'Spent' offences: As we have indicated, from the time that a child enters the lowest levels of the youth justice system, information will have been circulated in multi-agency arrangements. The Rehabilitation of Offenders Act allows convictions that resulted in less than 2.5 years custody (most young offenders) to become "spent" so that they no longer have to be declared (e.g. when applying for a job), although they will always remain on the Police National Computer. For young people the time period varies between 6 months and 5 years depending on the seriousness of offence. There is considerable concern as to whether the large number of systems described or referred to in this report all enforce the rehabilitation rules correctly; not to do so must, we believe, contravene data protection law unless there is a specific statutory provision to the contrary.

Chapter 6. Health Systems

As noted above, the NHS has been a pioneer in what is now called 'e-government' with its information management and technology programme. This started in 1992 with the aim of building for each patient 'a unified electronic patient record, accessible to all in the NHS'. This ran into opposition from the BMA in 1995–6 when doctors realised the implications for patient privacy and professional autonomy; the result was a 1997 enquiry by the Caldicott Committee leading to a report that documented the systems that existed, or that were being built, to share personal medical information between various providers, purchasers and other bodies within the NHS.[109]

Starting in 2002, the Government has launched the National Programme for IT (NPfIT), a large modernisation and centralisation initiative based on the 1992 vision. The debates over health privacy versus systems integration have not been resolved; there is still tension between GPs and the Department of Health over consent, central data collection and other issues. A celebrated case (described below) led ministers to promise that patients unhappy with central collection of their personal medical information will be able to opt out. GPs are still pushing for an "opt in" system instead, and are withholding cooperation from the computerisation program. This continuing debate may be a harbinger of the troubles in store for children's databases in the future.

However, the story of the health privacy debate is well known to the Information Commissioner, and health systems are not a focus of this research report. In this section we therefore present a more abbreviated summary of the main systems holding personal medical information in the UK. Their significance in this context is the participation of doctors – most importantly GPs and A&E staff – in child protection and in the investigation of allegations or suspicions of abuse. There is thus the possibility that information will flow between medical systems and other children's systems, with the resulting implications for privacy, data protection and consent.

6.1 Core Administrative Systems

The NHS-Wide Clearing Service (NWCS)[110] processes claims from health providers such as hospital trusts to purchasers such as Primary Care Trusts (PCTs) for payment. A typical record refers to a "finished consultant episode" and contains information such as the patient's name, diagnosis, treatment and cost. These records cover both in-patient and day care, and include many of the most privacy-sensitive medical facts (such as terminations of pregnancy). The scope of the service has been continually widened, with outpatient attendance added in 2001, mental health in 2003 and A&E attendance in 2005.

Although originally designed to deal with payments following the introduction of the

[109] The Caldicott Committee, 'Report on the Review of Patient-Identifiable Information', Department of Health, December 1997

[110] See http://www.connectingforhealth.nhs.uk/nwcs, accessed February 17 2006

purchaser/provider split in the NHS, NWCS has developed many secondary uses over the years. The first was the Hospital Episode Statistics (HES) database,[111] used for planning, audit etc; recently the NWCS has been developing a "Secondary Use Service" which aims to centralise and rationalise secondary uses of personal health information in the UK. It will 'provide timely, pseudonymised patient-based data and information for purposes other than direct clinical care, including planning, commissioning, public health, clinical audit, benchmarking, performance improvement, research and clinical governance.[112]

Other core administrative systems include those that map patients' names and addresses to NHS numbers and record the GP with whom a patient is registered. This used to be called the 'Administrative Register', which is the name still used in Wales. In Scotland it is called the 'Central Register' while in England the system was called the 'Strategic Trading Service' for a while, and is now the 'Personal Demographics Service' (PDS). As the NHS number is relied on for security in the NHS – some applications consider records to be de-identified and thus shareable without consent if identified only by NHS number – the NHS has refused to give social care systems access to NHS numbers. This in turn is one of the justifications for the existence of the ISA as a separate population index – and an example of the principle that problems often arise when a name in one system is used as a password in another.[113]

It is worth noting in passing that there has been much controversy (especially in the USA and Iceland) about the extent to which patients in supposedly de-identified databases can be re-identified. In practice, this is often easy when there are cognate sources of information on the data subject. One case is where someone with access to such a database knows a lot about the subject (e.g. a journalist writing about a celebrity); another might arise if someone used (for example) ICS data to access de-identified medical data.

6.2 NHS Care Records Service

The Care Records Service (CRS) has been the subject of a major systems development effort and has been described as implementing the 1992 vision of a single electronic medical record. The project is also scheduled to take over the secondary uses services from NWCS. As implementation has progressed, the description of the system has changed from a centralised database into a more federated system. Each patient will have a central 'Summary Care Record' with information such as allergies and medications, and pointers to 'Detailed Care Records' at provider organisations such as GPs' practices (or PCTs) and hospitals.

There is still considerable debate about who will have access to how much information, and what arrangements will be made for patient opt-out and indeed for the handling of

[111] See http://www.dh.gov.uk/PublicationsAndStatistics/Statistics/HospitalEpisodeStatistics/fs/en, accessed February 17 2006
[112] See http://www.connectingforhealth.nhs.uk/delivery/programmes/sus, accessed February 17 2006
[113] R J Anderson, 'Security Engineering – A Guide to Building Dependable Distributed Systems', Wiley, 2001

especially sensitive matters. The Department for Health insists that patients not wishing their data to be held on the system must opt out, and is planning a national campaign to persuade people not to do this; the BMA GPs' Committee is insisting that patients should have to opt in.

6.3 Prescription Data

The Prescription Pricing Authority in Newcastle holds records of all prescriptions fulfilled in England. Data are collected from pharmacies and made available to the prescribing GPs for verification of compliance, budgetary control and so on. Various central bodies also obtain data for secondary purposes. Since 1996, the police have apparently obtained data on opiate prescriptions, supposedly so that mis-prescribing can be investigated (unfortunately, this did not stop Harold Shipman). No patient consent is sought for these systems and no opt-out is available.

A new development is the electronic transmission of prescriptions. This enables a prescription to be sent directly to a pharmacist, and removes the need for patients to attend a surgery to obtain a simple repeat prescription.

6.4 Provider Systems

Healthcare providers such as GPs and hospitals maintain their own electronic record systems, many of which are largely computerised. There are a number of suppliers, although system functionality has generally been converging. In a general practice, the default is that all staff have access to all patients' records, while special arrangements may be made for patients with particular privacy needs (such as celebrities or family members of practice staff). These range from paper records through access controls to encryption.

In secondary care, some systems allow all hospital staff to see all records, though this has led to problems in the past, and some of the better systems provide properly-designed access controls. A standard way of doing this is controlling access by department; rules might state, for example, that every nurse has access to the records of any patient who has been in her ward during the previous 90 days, that every junior doctor has access to the records of any patient who has been treated in his department, and that consultants can also obtain the records of any other patient.[114]

There are lateral information flows between provider systems, such as electronic pathology messages that transmit lab test results from hospitals to GPs' surgeries.

[114] I Denley, S Weston-Smith, 'Privacy in clinical information systems in secondary care', BMJ 1999;318:1328-1331 (15 May)

6.5 Disease Management Systems

There are significant further lateral flows of data associated with specialist systems for particular patient groups – such as diabetes systems that facilitate cooperation between GPs and diabetologists in patient management. There have been tussles over control of these systems between primary and secondary care.

Of more concern here are the cases in which the tussles have engaged the patients on the one hand and the public health authorities on the other. For example, the Public Health Laboratory Service collected extensive information on sufferers from HIV/AIDS, which was represented as de-identified but was in practice re-linked by the PHLS system. The stated justification for this was getting an accurate measure of the number of people infected with HIV in Britain (as sufferers sometimes attended multiple clinics in different locations). The Caldicott Committee acknowledged that de-identification is difficult; in practice there are many ways in which supposedly anonymous data can be re-identified. Yet the practice continues of claiming, in some applications, that medical records identified only by NHS number are not 'personal data', with the consequences described above for sharing of NHS numbers with social care.

6.6 Secondary Uses

Overall, the control of access to information is good in the context of direct care (though improvements are definitely possible). The main privacy and data protection issues arise in the context of secondary uses, dozens of which were documented by the Caldicott Committee, and which continue to cause conflict to this day.

The information in provider systems is widely used for purposes such as research and clinical audit, although this usage is more pervasive in hospitals than in general practice. There are also many specific information flows to the centre that support particular public health purposes (such as immunisation), contractual aspects (such as item-of-service payments to GPs) and statutory reporting requirements (such as relating to notifiable diseases).

One data subject (Helen Wilkinson-Makey) was a GP practice manager who noticed untrue information about herself on a central system to which she had access: in particular there was an incorrect diagnosis of herself as an alcoholic. She pursued a complaint with the help of her MP to the point of receiving ministerial assurance that she could be treated on the NHS without having her information lodged on central systems. It is by no means clear how the NHS would cope with a large number of patients who opted out; how for example would payments for their treatment be processed? This issue had in fact already been raised by the BMA in 1996 but brushed aside by the Department of Health.

Other data subjects object on grounds of principle to their data being used for research purposes, for example in the development of contraceptives or abortifacients. In many cases, no opt-out is available: to give just two recent examples, the Health Service

(Control of Patient Information) Regulations 2002 asserted central access to all records on cancer, while the Health and Social Care (Community Health and Standards) Act of 2003 allowed the Secretary of State access to all UK health records for the purpose of 'health improvement'.

There are also ownership issues. GPs had long owned their computers and been considered the controllers of that data, but the 2003 General Medical Services contract started a move to computer ownership by Primary Care Trusts. This may interact with the proposed IS and ICS systems. For example, a typical GP would not consider it ethical to share an early diagnosis of hyperactivity, as it is not a notifiable disease and the risk of stigmatisation is clear. If such personal health information ends up being harvested only from those practices that have their record systems hosted at the PCT, this may fuel further confrontation between medical practitioners and the NHS over patient confidentiality, and even undermine medics' confidence in social services.

6.7 Summary

The history of healthcare IT in Britain may hold some useful lessons for people building social care and criminal justice systems that assume large-scale data sharing and integration. Fifteen years, and many billions of pounds, have been spent on computerising the health service, but with mixed results and rather limited professional buy-in. A forthcoming report from the National Audit Office (to which some of the current authors contributed) offers a comparative analysis of healthcare IT performance in the UK versus several European countries and the USA. At the time of writing, that report has still not been published.

However, if we had to suggest a single cause for the mediocre performance of healthcare IT in the UK, it would be the attempt to use massive IT investments as a means of driving change and reform. It is widely recognised that healthcare is less efficient (and uses IT less) than other service industries such as banking. However, there are good reasons for this: healthcare is complex, efficiency gains depend on improving working practices, and IT is not a good substitute for needed reform. Other countries have set out to create the 'electronic health record' via an incremental program of pushing interoperability standards and developing messaging, while leaving the underlying data largely with provider systems. System development is more evolutionary, and driven by the real needs of the users. Our colleagues overseas therefore watched with interest and trepidation as the UK set out on a 'moon-shot' approach of replacing existing systems with a centralised system, with the National Programme for IT and the early designs for CRS. However, for purely pragmatic reasons the CRS is now mutating more into a spine that will link up existing provider systems.

It remains to be seen whether social care systems will follow a similar evolutionary path, from an initial 'big-bang' national project to a more federated approach. It also remains to be seen whether the use of poor privacy mechanisms will become entrenched, such as the reliance on NHS numbers for anonymity by some health systems.

Chapter 7. Legislative Background

In this chapter,[115] we provide an outline and assessment of the legislative and regulatory framework for the data collection and sharing discussed in this study. In section 7.1, we will set out the general UK and European framework for this processing. In section 7.2, we summarise the statutory powers on which the databases and data sharing arrangements described in chapters 3–6 are based. In section 7.3, we will set out our conclusions as to the compatibility of the databases and associated data sharing arrangements described in chapters 3–6 with the relevant UK and European data protection standards.[116]

7.1 The Data Protection Framework

In the UK, as in other European countries, privacy rights are guaranteed by a patchwork of European, national and case law. In line with the EC directive that it seeks to implement,[117], the Data Protection Act 1998 (DPA98) sets out a number of basic data protection principles, as well as a series of general conditions for lawful processing of ordinary (non-sensitive) personal data and a series of special conditions for the processing of "sensitive" data (such as data on religious beliefs, sexual life, health, or criminal convictions).[118] Basically, all processing of personal data must (a) comply with

[115] This section draws on the Department for Constitutional Affairs' Public Sector Data Sharing: Guidance on the Law, November 2003, which is part of the DCA's "data sharing toolkit" and can be found on the DCA's website at: http://www.dca.gov.uk/foi/sharing/toolkit/lawguide.htm#part7, and on the country report on the United Kingdom in: D Korff, Data Protection Laws in the European Union, Brussels/New York, 2005. The former (hereafter referred to as "the DCA guidance"), according to the Secretary of State for constitutional affairs, Lord Falconer, "represents the consensus of legal opinion across Government" on the issue (Foreword). It is more detailed than any guidance issued by the Information Commissioner, and in particular than the Commissioner's more general Data Protection Act 1998: Legal Guidance (referred to as "the ICO guidance"). The Commissioner was consulted on the DCA's guidance (para.1.6).

[116] Reference is made to European, as well as UK standards because the relevant UK rules (in particular, the Data Protection Act 1998 or DPA98) are either specifically intended to apply European rules (in particular, the EC Framework Directive on data protection, Directive 95/46/EC) and/or touch on fundamental rights protected by the European Convention on Human Rights (ECHR), in particular, Article 8, which guarantees inter alia respect for private life. They must therefore, under the European Communities Act (ECA) and the Human Rights Act (HRA), be applied in a way that is compatible with these European standards. In theappendix, we will discuss how some other European countries, with a longer history of data protection, address similar issues within this same European context.

[117] Directive 95/46/EC of the European Parliament and the Council of 24 Octoer 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. The directive is hereafter referred to as "the Framework Directive" because it sets the framework for EC data protection law generally: several subsidiary directives have been adopted, which apply subject to the general principles of the Framework Directive.

[118] The principles were already contained in the 1982 Convention on data protection and in the DPA84, but the conditions were new to both the Framework Directive and the DPA98. The principles are set out in Schedule 1, Part I, to the 1998 Act; the interpretative provisions in Schedule 1, Part II. The general conditions for lawful processing are set out in Schedule 2; and the special conditions for the processing of sensitive data in Schedule 3. This report will not discuss the contentious issue of what exactly constitutes "personal data" because it is accepted by all the organisations involved in the arrangements discussed in

the data protection principles and (b) be based on one of the relevant conditions (i.e. on one of the general conditions for processing of non-sensitive data, and, where appropriate, on one of the special conditions for processing of sensitive data). The 1998 Act adds certain interpretations to the principles which are not contained in the Directive and also links the principles and the conditions in ways that could inadvertently lead to interpretations of the Act that are inconsistent with the Directive – and thus, possibly, with the European Convention on Human Rights (ECHR) and the Human Rights Act 1998 (HRA). As we shall see, this has important implications.

The Data Protection Principles

The DPA98 sets out the five data protection principles, contained in Article 6 of the Framework Directive, in the first five paragraphs of Part I of a special schedule (Schedule 1) to the Act, in terms close (but not quite identical) to those used in the Directive.[119] Put simply, personal data must be:

- processed fairly and lawfully (the first principle);
- processed only for specified and lawful purposes, and not further processed in any manner incompatible with those purposes (the second principle);
- adequate, relevant and not excessive in relation to those purposes (the third principle);
- accurate and kept up to date (the fourth principle); and
- not kept for longer than necessary to achieve those purposes (the fifth principle).

The most important principles for the purpose of this study are the first and second; the third, fourth and fifth principles are linked to the second principle.

Fairness and Lawfulness

The overriding principle is "fairness", which in the Directive is stipulated without further comment, but to which the DPA98 adds extensive gloss. Thus, first of all, the Act adds to the principle that "personal data shall be processed fairly and lawfully" the words: "and, in particular, shall not be processed unless [one of the general or, for sensitive data, one of the special conditions] is met" (Schedule 1, Part I, first principle). Secondly, Part

---

this report that the data they share on children and young people are "personal data" within the meaning of the Act. For a critical discussion of the position adopted by the UK courts on that question in the Durant case, see "Paper No. 4: The Legal Framework – an analysis of the 'constitutional' European approach to issues of data protection and law enforcement" in: I Brown and D Korff, Privacy & Law Enforcement, study for the Information Commissioner, 2004.

[119] The Act also includes in the list in Part I of Schedule 1 a sixth principle, stipulating that personal data "shall be processed in accordance with the rights of data subjects under this Act"; a seventh principle requiring the taking of "appropriate technical and organisational measures" to ensure data security; and an eighth principle that prohibits the transfer of personal data to a non-EU/EEA country that does not ensure "adequate protection." In the Directive, these matters are not dealt with as data protection principles, but as separate substantive matters.

II of Schedule 1 to the Act contains no less than four provisions "interpreting" the fairness principle, three of which are relevant to this study.[120]

The first provision (contained in Schedule 1, Part II, para.1(1)) stipulates quite generally that:

> *In determining for the purposes of the first principle whether personal data are processed fairly, regard is to be had to the method by which they are obtained, including in particular whether any person from whom they are obtained is deceived or misled as to the purpose or purposes for which they are processed.*

Furthermore, the second provision (contained in Schedule 1, Part II, para.2) links the question of "fairness" more specifically to the duty to inform data subjects of various matters (such as the purposes for which their data are to be used), in the sense that "personal data are not to be treated as processed fairly" unless these informing requirements are met. It should be stressed that these clarifications should not be read as suggesting that as long as there was no deception, and as long as the information duties are fulfilled, the processing in question is "fair". In fact, "fairness" can relate to any matter, including but not limited to these matters.

On the question of "lawfulness", guidance from the Department for Constitutional Affairs (DCA) links this to four legal issues which we shall discuss later, in the section on data sharing on the basis of statutory provisions:

> *"Under the first Data Protection Principle, personal data are required to be processed 'fairly' and 'lawfully'. The requirement that the personal data be processed 'lawfully' means that those legal obligations both statutory and common law must be complied with. The DPA cannot render lawful any processing which would otherwise be unlawful. In the context of public sector data sharing this means that the public body must have the vires to carry out the processing (or the function to which the processing of the data is ancillary), that the processing is not in breach of the law of confidence, that the processing is not in breach of any other relevant domestic statute or common law principle, and that it is compliant with the HRA, the ECHR (Article 8 in particular) and any applicable principles of EU law. Accordingly, the DPA overlaps with other areas of law."* [121]

Purpose Specification and Limitation

The second data protection principle set out in Schedule 1, Part I, of the DPA98, reads as follows:

---

[120] The final interpretative clause relates to the use of "general identifiers" such as a national identity number or national insurance number. It may suffice to note here that the Secretary of State can issue an order setting out the conditions for the use of such numbers, and that in fact the stipulating of such conditions is required under the Framework Directive – but that no such order has as yet been issued.
[121] DCA guidance para. 6.5.

Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

The Act does not specify how precise the "specification" of the "specified purpose" should be. As will be shown in the appendix, this is seen as a crucially important matter in other European countries: it largely determines whether the third, fourth and fifth principles are complied with. As noted below, in the discussion of the conditions for lawful processing, it may also determine whether the information given to data subjects is sufficient and whether any "consent" is valid (and it should indeed play a role in assessing whether processing is "fair" in respect of the data subject).

The standard categories used for notification will not always be sufficient. The ICO list itself makes this clear: for example with regard to the purpose defined as "research", the ICO adds that the controller "will be asked to indicate the nature of the research undertaken". As concerns "education", the ICO merely observes that this covers, "the provision of education or training as a primary function or as a business activity", The ICO list of standard purposes does not include social work (let alone youth social work).

One of the main issues identified earlier in this report is the shift in meaning of the term "at risk" as used in work with children, from "at risk of significant harm or neglect" to "at risk from failing to achieve the government's five targets for children" and "at risk of social exclusion". If the purpose of data collection, processing and sharing is defined as "protecting children at risk" in these very broad senses, then clearly this shift in meaning leads to a major widening of the "specified purpose" for which the data are processed. The question then arises whether the wider purposes are still sufficiently specific in terms of the DPA98.

To the extent that a purpose may be set out in law (in a statute or in an instrument adopted under a statute), the question of its required specificity also again relates to the question of the "quality" of that law in terms of the ECHR/HRA. The DCA clearly recognises this in its legal advice:

> *"It is a matter of statutory construction as to whether a particular statutory gateway authorises disclosure for the particular purpose or purposes contemplated. In construing the statute account must be taken of the HRA and of the DPA."* [122]

We will return to this below, in our discussion of the conditions for lawful processing

With regard to the question of "compatibility", the 1998 Act significantly tightens the law compared to the 1984 Act. The earlier Act linked the question of compatibility (in the view of the Data Protection Registrar at the time, "irrationally") with the question of

[122] DCA guidance para.3.15. The term "statutory gateway" is used to describe statutory provisions (or provision in subsidiary regulations) requiring or authorising disclosures of data: see section 3, below.

registration: if a certain secondary purpose was notified to the Registrar, its compatibility with the registered primary purpose could not be challenged. Under the 1998 Act, by contrast, the Information Commissioner has the power to take enforcement action if he feels that "incompatible" processing occurs. His guidance states, inter alia, that:

> *Where the data controller already holds information obtained for a specific purpose, it can only be used for a different purpose that would not have been envisaged by the data subject at the time of the collection of the information if the data controller has the consent of the data subject.*[123]

Many if not most secondary uses of the data discussed in this report will require consent. We will now examine this in more detail.

Conditions for Lawful Processing

As already noted, the DPA98, in line with the Framework Directive, sets out (in Schedules 2 and 3, respectively) a series of general conditions for the processing of personal data, and a series of (stricter) special conditions for the processing of "sensitive" data. For processing of non-sensitive data, one or more of the general conditions in Schedule 2 must be met; for processing of sensitive data, one of the special conditions in Schedule 3 must be met. The general conditions broadly correspond to what are called "criteria for making data processing legitimate" in Article 7 of the Framework Directive; the special criteria broadly correspond to what are framed as exemptions from an in-principle prohibition on the processing of sensitive data in Article 8 of the Directive.

For the purpose of this study, two types of condition are important: processing on the basis of "consent" and processing on the basis of statutory authority (often referred to in the UK as "statutory gateways").

Collecting, Processing and Sharing of Personal Data on the Basis of Consent

Under the DPA98, processing of non-sensitive data is always allowed with the consent of the data subject (Schedule 2, para.(1)). Processing of "sensitive data" requires "explicit consent" (Schedule 3, para.(1))[124] – but the term "consent" is not defined in the Act. However, since the Act implements the Directive, the term in the Act must be read in accordance with the definition of consent in that instrument:

> *'the data subject's consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.* (Art. 2(h) of the Framework Directive)

[123] ICO guidance, section 3.1.7.3, on pp. 32 – 33.
[124] The Framework Directive allows States to prohibit processing of sensitive data in certain context, even with the consent of the data subject, but the UK has not availed itself of this. For an example of such a provision in France, see the appendix.

In addition, the Directive stipulates that consent, if used as a condition for processing, even of non-sensitive data, has to be given "unambiguously" (Art. 7(a)).

This means that consent, even for the processing of non-sensitive data, can only be regarded as valid if the data subjects were informed in clear and precise ("specific") terms about the intentions of the controller – and of course in particular, about the purpose(s) for which their data are to be used and about any intention to share their data, and if so, with whom and for what purposes[125] – and if they were competent and free to agree or not to agree to the proposed uses or disclosures. This is reflected in the guidance of the Information Commissioner on consent, in particular in relation to processing of sensitive data:

> *The adequacy of any consent or purported consent must be evaluated. For example, consent obtained under duress or on the basis of misleading information will not be a valid basis for processing.*
> *...*
> *Consent must be appropriate to the particular circumstances. For example, if the processing is intended to continue after the end of a trading relationship then the consent should cover those circumstances. However, it must be recognised that even when consent has been given it will not necessarily endure forever. While in most cases consent will endure for as long as the processing to which it relates continues, data controllers should recognise that, depending upon the nature of the consent given and the circumstances of the processing, the individual may be able to withdraw consent.*
> *...*
> *There is a distinction in the Act between the nature of the consent required to satisfy the condition for processing and that which is required in the case of the condition for processing sensitive data. The consent must be "explicit" in the case of sensitive data. The use of the word "explicit" and the fact that the condition requires explicit consent "to the processing of the personal data" suggests that the consent of the data subject should be absolutely clear. In appropriate cases it should cover the specific detail of the processing, the particular type of data to be processed (or even the specific information), the purposes of the processing and any special aspects of the processing which may affect the individual, for example, disclosures which may be made of the data.* [126]

The next questions are when a person, and in particular a child or young person, can be said to be competent to give the required (specific and informed) consent, and when they can be said to have given consent "freely".

---

[125] cf. DCA guidance para.6.8 on p. 25. The Information Commissioner also stresses that "The data controller must always be open [viz-à-viz data subjects] about what personal data will be collected, the purpose(s) it will be used for, who it will be disclosed to and under what circumstances those disclosures will be made."

[126] ICO guidance, para.3.1.5, on pp. 29–30. Note that the Commissioner too in this regard specifically and expressly draws on the definition of consent in the Framework Directive.

Valid Consent and Competence to Give Consent

The Department of Constitutional Affairs does not take issue with the IC's guidance, but does not elaborate it either:

> *As a general rule the Information Commissioner has indicated that consent should be 'informed' and 'unambiguous'. Consent is notoriously hard to define, although most people (we imagine) would feel able to recognise it when they saw it. An evaluation of the adequacy of consent in the circumstances where it is not obvious that it has been given or that it is fully 'informed', make it difficult to generalise. [sic]* [127]

It is however notable that the Department feels that consent need only rarely be relied on:

> *However, in the context of public sector data sharing that is intra vires it is likely that the processing involved will meet at least one of the conditions in Schedule 2 or Schedule 3 mentioned above and, where this is the case, consent is not a necessary precondition.* [128]

The Information Commissioner has not, as yet, issued any specific guidance on the capacity of children and young persons to give valid consent for processing. However, he has issued some guidance in connection with the issue of subject access, and more generally on the question of when parents should be involved or may access information on their children. In the context of this study, the Office of the Information Commissioner told us that "although the legal guidance concentrates mainly on the circumstances surrounding subject access requests, the underlying principles are the same in general for almost all circumstances." More specifically, we were given the following outline of its position:

> *If a data subject is of sufficient maturity to understand their rights under the Act then the data subject should be approached for consent to process their personal data. In general the Commissioner believes that at the age of 12 an individual is likely to have this level of maturity, but understands that this may not always be the case. If there is reason to believe that the data subject does not have this level of maturity then the data controller may approach another (appropriate) individual for consent. However, even a data subject who does have the required level of maturity to act on their own behalf may, if they wish, designate someone to act as their representative.*
> ...
> *There does appear however, from time to time, to be some confusion in the matter of consent in schools. This usually relates to the age of pupils and the point in time when educational establishments should cease to ask parents' consent to process pupils' personal data and should start to ask the pupils themselves.*
> …

[127] DCA guidance para.6.21 on p. 27.
[128] Idem.

For example the Learning and Skills Act 2000, which makes the provisions under which Connexions operates, quotes 16 as the age at which the pupil should give consent for their personal data to be passed on to their local Connexions group. For anyone below that age the parent is expected to offer, or refuse, consent.

In addition the Education (Pupil Information) (England) Regulations 2000 (SI 297 of the Education Act 1996) offers parents a statutory right of access to some, strictly limited, information which schools hold about their children, whether the child consents or not. [129]

The question of consent is linked to the question of "Gillick competence". We therefore explain this, then discuss the question of when consent can said to be "freely given". Finally, we will briefly discuss when (if ever) personal data on third parties (parents, siblings, friends, etc.) can be based on the consent of a data subject (especially if that data subject is a child).

Gillick Competence

The question as to whether children can consent to procedures that affect them has been considered in the medical field. Section 8 of the Family Law Reform Act 1969 provides that those aged between 16 and 18 can consent for themselves to medical procedures. The position of those under 16 was considered in the well-known case of Gillick v West Norfolk and Wisbech Area Health Authority,[130] the principles of which have been distilled from the leading speech of Lord Fraser and are commonly referred to as the "Fraser Guidelines". These set out criteria for doctors and other health professionals to apply in ascertaining, where there is a conflict of interest between a child or young person and his/her parents, whether medical advice or treatment can be given without the consent or knowledge of the parent. A child or young person who is judged after consideration of these criteria as having the capacity to consent is often referred to as being "Gillick competent".

We are aware of instances where data have been gathered and shared by various practitioners (not just health professionals) without consideration of parental consent, on the basis that the child or young person under 16 is "Gillick competent". Whether this is a correct approach has not been specifically determined by a court and merits further attention.

It is necessary to start with a consideration of the background to cases such as Gillick, which has recently been considered and adhered to in R (on the application of Sue Axon) v Secretary of State for Health.[131] In those cases, the Department of Health offered confidential advice on contraception and abortion to young people under 16 who were assured that their parents would not be informed. Mrs Gillick and Ms Axon were parents

[129] Letter from the Office of the Information Commissioner of 25 January 2006.
[130] Gillick v West Norfolk and Wisbech Area Health Authority [1985] 3 All ER 402.
[131] R (on the application of Sue Axon) (Claimant) v Secretary of State for Health (Defendant) & Family Planning Association (Intervener) [2006] EWHC 372 (Admin).

who objected to this, believing that any such treatment should not only be disclosed to parents but required their consent.

In Gillick, the House of Lords (by a majority of 3 to 2) held that parental consent was not required, and Lord Fraser propounded guidelines establishing the procedure to be followed when a child or young person sought confidential medical advice:

1. if a doctor was of the view that the procedure could be said to be in a child's best interests, and

2. if that doctor could not persuade the child to tell her parents, then

3. provided that the child was able to understand the nature and consequences of the medical procedure:

the child was competent to consent without the knowledge and consent of her parents.

This formula has been applied by professionals dealing with children and young people in other areas where consent is necessary. As we have noted, some agencies believe that a child or young person is able to consent to have his/her data collected and shared without parental involvement, knowledge or consent if the child is said to be "Gillick competent". A "Gillick competent" child or young person is then said to be one who is possessed of the intelligence and maturity to be able to understand the nature and consequences of the choice being put to them. This "test" appears to concentrate on only one aspect of the criteria referred to in the Fraser Guidelines, and carries with it the possibility that the other considerations are forgotten. If this part is taken out of its context, are the Fraser Guidelines being followed?

It is instructive to set out in full the relevant passage of Lord Fraser's speech in Gillick:

> *The only practicable course is to entrust the doctor with a discretion to act in accordance with his view of what is best in the interests of the girl who is his patient. He should, of course, always seek to persuade her to tell her parents that she is seeking contraceptive advice, and the nature of the advice that she receives. At least he should seek to persuade her to agree to the doctor's informing the parents. But there may well be cases, and I think there will be some cases, where the girl refuses either to tell the parents herself or to permit the doctor to do so and in such cases, the doctor will, in my opinion, be justified in proceeding without the parents' consent or even knowledge provided he is satisfied on the following matters:*
>
> *(1) that the girl (although under 16 years of age) will understand his advice;*
>
> *(2) that he cannot persuade her to inform her parents or to allow him to inform the parents that she is seeking contraceptive advice;*

(3) that she is very likely to begin or continue having sexual intercourse with or without contraceptive treatment;

(4) that unless she receives contraceptive advice or treatment her physical or mental health or both are likely to suffer;

(5) that her best interests require him to give her contraceptive advice, treatment or both without the parental consent.

That result ought not to be regarded as a licence for doctors to disregard the wishes of parents on this matter whenever they find it convenient to do so. Any doctor who behaves in such a way would be failing to discharge his professional responsibilities, and I would expect him to be disciplined by his own professional body accordingly. [132]

In addition to a child or young person understanding the nature of her choice, there is considerable emphasis on the requirement that she be encouraged to involve her parents. It has also to be remembered that the court takes it for granted that the medical professional, in accordance with professional obligations, makes a full and detailed explanation of the procedure, its advantages and disadvantages, to the young person.

Is this the position when a child or young person is asked to give consent to data sharing? In the Gillick situation, the child or young person herself is asking for provision to be made without the knowledge of her parents as there is a perceived conflict. The guidelines are designed to inform doctors as to how to resolve that conflict when it exists; the emphasis on involving parents makes that abundantly clear.

While we all take for granted that advice provided by a medical professional will be impartial, can the same be said of a practitioner in an agency where information-sharing is considered an essential component of the service? In that situation there is inevitably an institutional bias towards gaining consent.

Where a child or young person is asked for consent where there is no conflict of interest, there is no reason or necessity, and therefore no justification, for dispensing with parental consent, or involvement. Indeed, if consent of children or young people is being sought on the basis of convenience without the encouragement of parental participation, that would appear to be capable of amounting, as Lord Fraser sets out, to a failure in the professional to "discharge his professional responsibilities".

In the later case of Axon (2006), Silber J said:

The basis of the Gillick decision was that a doctor's duty vis-à-vis the girl's parents was initially to "seek to persuade the girl to bring her parents into consultation" (per Lord Scarman at page 189E) and "always seek to persuade [the girl] to tell her parents that she is seeking contraceptive advice, and the

[132] Gillick v West Norfolk. Since the case concerned a girl, the references are to "her" only.

> *nature of the advice she receives" (per Lord Fraser at page 174E). If those attempts failed, then the majority decision in Gillick allowed the medical professionals to provide contraceptive advice and treatment subject to certain important conditions being complied with.* [133]

It should also be remembered that the situation considered by Lord Fraser was one that concerned consent in a specific, time-limited situation. By contrast, the consent that is sought for data-sharing in the cases examined in this study is often of a more general nature in that it is intended to allow a range of practitioners access to a database or other record of information about a child over a long period of time, for a wide range of purposes which may not be all apparent at the time consent is sought. This "blanket" consent may be taken once only, and the young person may not necessarily be able to specify the people who may (or may not) access the record, nor the circumstances in which they may do so.

For example, when asked about the rights of young people in relation to information held on the Connexions database, the Minister for Schools replied:

> *Young people have the right to see all information held about them by Connexions, and are able to request correction of any inaccurate data. They are not able to control access to Connexions partnerships' databases.* [134]

At the time when a young person using the Connexions service gives consent, s/he may be entirely willing to have information about a specific problem disclosed to others; but it is another matter entirely to assume that s/he is also capable of consenting simultaneously to having details of unimagined situations that may develop in the future accessed by several practitioners, or of understanding the possible ramifications of having given such consent. The implications of a single consent to multiple and future acts of data-sharing are far more complex than the situation envisaged in Gillick.

Earlier, we quoted the Commissioner's comment that "it must be recognised that even when consent has been given it will not necessarily endure forever".[135] This too clearly has a bearing on the topic of this study.

Of tangential interest to the above discussion is the case of Mabon v Mabon[136] which arose out of a dispute between separated parents as to the residence of their children. The Court of Appeal considered whether Rule 9.2A of the Family Proceedings Rules 1991 applied to three brothers aged 17, 15 and 13 who wished to dispense with the services of their guardian ad litem in order to participate directly in the court proceedings. The Court held that Salisbury County Court had been "plainly wrong" in rejecting the boys' application to instruct solicitors on their own behalf.

---

[133] Silber J. in R (on the application of Sue Axon), at para.61.
[134] Commons Hansard 20 March 2002: Column 341W.
[135] ICO guidance, para. 3.1.5, on p. 29.
[136] Mabon v Mabon [2005] EWCA Civ 634.

Lord Justice Thorpe, in giving judgment, stressed the importance of focussing on a child's sufficiency of understanding:

> *"…and, in measuring that sufficiency, reflect the extent to which, in the 21st Century, there is a keener appreciation of the autonomy of the child and the child's consequential right to participate in decision making processes that fundamentally affect his family life"*

However, the Mabon judgment deals with the capacity of children to take part in court proceedings rather than with the issue of consent, and while it is helpful when assessment of Gillick competence becomes necessary, it has no bearing on Lord Fraser's guidelines concerning the pre-existing circumstances in which such an assessment may occur. The child's right to consult parents before making decisions is absolute, and it is only when the child actively indicates that s/he does not wish to exercise that right that an assessment of competence to give consent should take place.

Free Consent

As noted earlier, a further crucial matter is the question of when consent can be said to be "free". As the Information Commissioner's Office puts it:

> *Consent should always be freely given, thus any document prepared by the data controller to obtain consent should not contain any coercive element, and lack of consent should not generally cause any detriment to the individual, particularly in respect of any statutory rights that individual has.* [137]

In fact, the issue of course extends beyond the contents of any "consent form". All the circumstances surrounding the obtaining of consent should be taken into account – and there is, as concerns children and young people, a strong interplay with the question of competence.

Specifically, we noted that there are already serious legal questions of when children and young people are generally competent to give consent to the processing of highly sensitive data on them. Unless under-16s have been invited to involve their parents, these questions become sharper if the data are to be used for a wide range of not-very-clear, or at least very-broadly-defined purposes, and sharper still when the context in which they are asked to provide this "consent" is such as to make it difficult for them to refuse.

First, the practitioners asking the young people for consent may have access to them in an environment where they are habituated to co-operate with the wishes of adults (such as at school). This would not seem to be an environment conducive to genuinely free choice.

[137] Letter from the Office of the Information Commissioner of 25 January 2006. As noted earlier, the general ICO guidance merely says that "consent obtained under duress or on the basis of misleading information will not be a valid basis for processing."

Second, the young people may be told that providing the information is in their own interest, and that they may not be able to obtain the full range of "services" they might otherwise get should they fail to consent. These pressures, applied to vulnerable young people who may well need help, further undermine the validity of any "consent" thus obtained.

Officers for all of the UK Commissioners for Children and Young People have expressed serious concern about the implications for children's privacy of multi-agency data-sharing, about the use of blanket consent that allows multiple agencies access to a child's electronic records, and about the whole issue of using informed consent for complex issues of data-sharing.

In the circumstances, it would appear that closely involving, and informing, parents (rather than, as at present, totally excluding them) would appear to be the least that is required. We will return to this in Chapter 9, and we examine the practice in other countries in the appendix.

"Consent" to the Sharing of Information on Others

In gathering information about a child or young person's life, data referring to other people, particularly other family members, are also collected. Indeed, such information is often expressly sought: many of the databases described here contain specific fields for information on third parties (parents, siblings, friends) and even require assessments of those third parties. For instance, the APIR document used by Connexions includes information on the capacity and parenting skills of parents, and on substance use by family members and friends of the child to which the document relates.[138]

It is not apparent that consent is sought from the person to whom such information refers, nor that any mechanism exists to inform them so they can check its factual basis. The problem is acute where an agency relies upon the 'consent' of a child to process such data, as parents will have no oversight of data collected about themselves or their other children.

Under the DPA98, consent for the processing of personal data can only ever refer to the processing of personal data on the person giving consent. A person cannot "consent" to the processing of information on another person. Processing personal information on parents, siblings and friends of a child, on the purported basis of the child's "consent", without either the consent of those other data subjects or some specific statutory authority (as discussed later), is quite simply unlawful.[139] We suggest that the Information

[138] See Chapter 3, above.

[139] There may be circumstances in which information on a third party is entirely incidentally included in a record on a data subject, but without the data being used in any way with reference to that third party. Arguably, there is then no processing of personal data on the third person, and the inclusion of the information is then not subject to the DPA98. Under the ruling in Durant, it could furthermore be argued that if the data on the third party did not impact on that third party's private life, the data were also not "personal data" in the sense of the DPA98 – but that argument is risky because the compatibility of Durant with the Framework Directive is highly doubtful, as discussed in "Paper No. 4: The Legal Framework – an

Commissioner's guidance should tackle both notification of, and fairness to, third parties more explicitly. We will return to this in Chapter 9.

The sensitivity of metadata

A question that arises with a number of children's systems, and particularly in the context of IS, is the sensitivity of metadata. For example, if the IS records that a child is a former patient of a mental health or substance abuse service, that mere fact enables a deduction to be made about a sensitive matter, namely the child's health.

There is a gap between the DPA and EU definitions of sensitive data. The former talks of "information as to" race, politics, religion, health, sex and so on; the latter talks of "data revealing" such matters. Experts have argued about whether a photograph of someone might be sensitive matter under the directive (it reveals race) but not under the DPA.

For present purposes, however, the matter has been settled by the House of Lords in Campbell v MGN Ltd[140]. The appelant was photographed leaving a meeting of Narcotics Anonymous. The Court of Appeal had found that the mere fact of the appelant's therapeutic relationship was no more than a "peripheral disclosure" and thus was not a breach of the duty of confidence the newspaper owed her. Their Lordships disagreed and found that the information was private. As Baroness Hale put it: "[It] was of exactly the same kind as that which would be recorded by a doctor on those notes: the presenting problem was addiction to illegal drugs, the diagnosis was no doubt the same, and the prescription was therapy, including the self-help group therapy offered by regular attendance at Narcotics Anonymous." Given that a social worker, doctor or teacher owes a very much greater duty of confidence to a child in their care than a newspaper does to a celebrity, it seems inevitable that the non-consensual disclosure of a sensitive therapeutic relationship would infringe the law of confidence, and data protection law.

Collecting, Processing and Sharing of Personal Data on the Basis of Statutory Authority: the Issue of "Statutory Gateways"

The DCA provided the following guidance on "How to approach questions about data sharing":

> *There is a straightforward sequence of consideration, which should enable a sound judgement to be made about the ability of a public body to share personal data in the public interest:*

---

analysis of the 'constitutional' European approach to issues of data protection and law enforcement" in: I Brown and D Korff, Privacy & Law Enforcement, study for the Information Commissioner, 2004. These arguments are in any case not relevant to the databases and data sharing arrangements examined in this study, because in those the data on third parties (parents, siblings, friends) are specifically used with reference to those third parties – e.g. in deciding whether social service should go and see the family; and they undoubtedly touch on highly private matters, such as possible drug abuse by those third parties. Also irrelevant for the purposes of this study are the alternative conditions in Schedule 2 and 3. The "balance" condition in Schedule 2, para.6 is, in particular, not applicable to the processing of sensitive data on third parties such as parents or siblings.

[140] [2004] UKHL 22

Establish whether you have the power to carry out the function to which the data sharing relates. In doing so it will be important to ascertain whether there are express statutory restrictions on the data sharing activity proposed, or any restrictions which may be implied by the existence of other statutory, common law or other provisions.

Decide whether the sharing of the data would interfere with rights under Article 8 of the European Convention on Human Rights in a way which would be disproportionate to the achievement of a legitimate aim and unnecessary in a democratic society.

Decide whether the sharing of the data would breach any common law obligations of confidence.

Decide whether the sharing of the data would be in accordance with the Data Protection Act 1998, in particular the Data Protection Principles. [141]

The guidance sets out the basic principles relating to each of these points in brief, and then expands on them in separate sections. We will briefly look at each of these points, but in a different order and depth.

Principles of administrative law relating to data sharing

On the first issue, the DCA guidance points out, in a brief comment under the heading "administrative law", that:

It is a well established principle [of administrative law] that express statutory powers should be interpreted so as to authorise by implication the performance of acts reasonably incidental to those expressly granted. This principle is reflected in section 111(1) of the Local Government Act 1972 that provides that local authorities are expressly empowered to do anything which is calculated to facilitate, or is conducive or incidental to, the discharge of any of their functions. [142]

It goes on to say the following:

There is no general statutory power to disclose data, just as there is no general power to obtain, hold or process data. As a result, it will be necessary to consider the legislation that relates to the policy or service that the data sharing supports. From this, it will be possible to determine whether there are express powers to share data, or whether these can be implied from the terms of the legislation. Clearly, express powers to share data give the highest degree of certainty, but it should be borne in mind that such express powers to share data

[141] DCA guidance para. 2.3.
[142] Idem, para. 2.6.

> *are relatively rare and tend to be confined to specific activities and be exercisable only by named bodies. Implied powers will be more commonly invoked. .* [143]

Thus, if a statute sets out a public function for a particular public body, then, under this test (and in the absence of any obstacles arising out of the other points), data can be disclosed to that body by another body if the data are either specifically needed for the performance of that function by the receiving body, or if they are "reasonably incidental" to that function.

It is however important in this to distinguish between statutory provisions which set out the general powers – the scope of the vires – of a public authority, and provisions which set out more specific functions of such an authority. The first are basically intended to ensure that matters falling within the broad ambit of the field of activity of the public authority will not be held to be ultra vires just because they are not specifically set out in statute. The latter enable an authority to carry out more specific acts. The test of whether a data disclosure is "reasonably incidental" can be properly applied to the latter. However, to apply them to the former would create a framework of such elasticity as to impose hardly any constraints at all.

Thus, for instance, section 2 of the Local Government Act 2000 allows every local authority "to do anything which they consider is likely to achieve... the promotion or improvement of the [economic, social and/or environmental] well-being of their area". This cannot be read as allowing, by itself, all data collecting, use and sharing that is "reasonably incidental" to "the promotion of wellbeing in the area" (unless it is specifically forbidden). Indeed, the plethora of more specific provisions allowing for the setting up of databases, and the detailed regulations issued in respect of databases, noted in the earlier chapters, underline that the government too clearly feels that vague and all-encompassing provisions do not suffice. As we shall see later, this is reinforced by the DPA98.

Confidentiality and data sharing [144]

The issue of when data that are subject to a duty of confidentiality may be shared is not at all straight-forward and very much depends on whether there is a special statutory exception and on the circumstances, i.e. on the relationship from which the duty of confidentiality arises, the nature of the data, and the purposes of the data sharing.

The Information Commissioner links the question of confidentiality to the first data protection principle, which stipulates that personal data must be processed "fairly and lawfully", and to the second principle, on purpose specification and limitation:

> *There are circumstances where an obligation of confidence arises between a data controller and an individual about whom information is recorded, for example, in*

[143] Idem, paras. 2.7–2.8 and 2.10.

[144] We are grateful for the assistance of Nick Bohm, General Counsel of the Foundation for Information Policy Research, for his input on this section.

relation to medical or banking information. The effect of an obligation of confidence is that a data controller is restricted from using the information for a purpose other than that for which it was provided or disclosing it without the individual's permission. It would be unlawful for a data controller to do this unless there was some overriding reason in the public interest for this to happen. Where such personal data are processed for a purpose other than that for which the information was provided, the processing is likely to be unlawful processing.
...
Where a public body obtains information of a confidential nature in order to carry out its statutory functions then processes that information for other purposes, there is likely to be a breach of the obligation of confidence to that individual, unless there is a good reason or some legal justification for using the information in that way.

Research carried out by the Commissioner indicates that individuals have a high level of trust in the manner in which their information will be held by public bodies and believe that it will not be passed onto anyone else, or used for any but the most limited purposes apart from the purpose for which the information has been given.

An individual's legitimate expectation as to how the information given to a public body will be used will, therefore, also be relevant in considering whether there has been a breach of the First Principle. [145]

Breaches of confidence may be justified in certain circumstances, but tests of necessity and proportionality must be applied in order to decide whether disclosure is justified in the public interest (in accordance with the ECHR and HRA, as discussed later). This indicates the need for consideration of the circumstances on a case by case basis, at a suitably senior administrative level, rather than disclosure as a matter of routine, as in the systems described in the earlier chapters. Staff whose training and experience are insufficient to enable them to resolve difficult cases under the law of confidentiality should be trained to recognise and refer them upwards even when the routine prescribes disclosure. Particular care is required if the public interest justification for a breach of confidentiality is that disclosure is in the interests of the individual whose confidence is to be broken: where that individual refuses to consent, the disclosure is a breach of his or her right to autonomy, a right which ought not to be lightly overridden merely on grounds of the youth of the individual. One cannot argue at the same time that children are competent to give consent for data sharing, but that if they refuse consent, their confidence can be overridden simply because of their youth.

We also draw attention to the fact that responsibility for a breach of confidence rests on the discloser, and that the discloser must therefore be sure of the facts and matters relied on to justify a disclosure. It is not a defence to a claim of breach of confidence or privacy

[145] ICO guidance, para.. 3.1.4. The paragraph omitted from this quote was set out earlier, under the heading "Principles of administrative law relating to data sharing"; it points out that processing in violation of a legal duty of confidence would be unlawful.

to show that the discloser reasonably believed that the circumstances were such as to justify disclosure if in fact they were not. Those asked to make disclosures should therefore pay close attention to the reliability of the evidence on which they are asked to act, especially where it comes from the person or body to whom the disclosure is to be made. To focus the minds of those involved on the importance of the matter, the person or body who provides the information on which a discloser is asked to rely might appropriately be asked to warrant the truth of the information provided and to indemnify the discloser against liability or loss resulting from a breach of the warranty. The systems described in earlier chapters do not appear to allow for this.

Data Protection Rules and Principles Relating to Data Sharing

Under the DPA98, both sensitive and non-sensitive personal data can be processed without the consent of the data subject, in particular, if one of the following conditions, contained in both Schedule 2 and Schedule 3 to the Act, has been met:[146]

- the processing is necessary for the exercise of any functions conferred on any person by or under any enactment (Schedule 2, para.5(b), Schedule 3, para.7(1)(b)); or

- the processing is necessary for the exercise of any functions of the Crown, a Minister of the Crown or a government department (Schedule 2, para.5(c), Schedule 3, para.7(1)(c)).[147]

Alternatively, sensitive data can be processed "in circumstances specified in an order made by the Secretary of State for the purposes of this paragraph" (Schedule 3, para.10). An order, the Sensitive Data Order 2000, has been issued under this provision. [148]

As discussed later in this section, the applicability of the Sensitive Data Order to the kinds of data collecting and sharing arrangements addressed in this study is very limited: the main bases for the processing of sensitive data associated with these arrangements are the two conditions set out in paras 5(b) and (c) of Schedule 2 and in paras. 7(1)(b) and (c)

[146] Non-sensitive personal data may also be processed if the processing is "necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract" (Schedule 2, para.3) or if it is "necessary for the exercise of any other functions of a public nature exercised in the public interest by any person" (Schedule 2, para.5(c)). The former is echoed in Schedule 3, para.2, but only in relation to employment, which is not relevant to this study; both conditions in any case only cover disclosures that are required, not disclosures under "permissive statutory gateways". There is no parallel to the latter condition in Schedule 3; it applies in particular to cases in which private-sector bodies (such as charities or private trusts) are charged with the carrying out of public functions, or contracted to carry out such functions. But since the data to be shared under the arrangements under consideration in this study all include sensitive data; they will not be further discussed here. It is in any case clear that, even for the sharing of non-sensitive data, the conditions discussed in the text are the main ones relied upon.

[147] A further condition, contained in both Schedules, is that the processing is "necessary for the administration of justice" (Schedule 2, para.5(a), Schedule 3, para.7(1)(a)), but this purpose is not at issue for the database and data sharing arrangements examined in this study.

[148] Full title: Tte Data Protection (Processing of Sensitive Personal data) Order 2000 S.I. 2000 No.417.

of Schedule 3, set out in the bullet-points, above. However, they are, from a European perspective, highly dubious.

Specifically, these two provisions correspond to the single criterion in Article 7(e) of the Framework Directive, allowing processing of personal data when this 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 or in a third party to whom the data are disclosed".[149]

However, that condition/criterion only applies to the processing of non-sensitive data. Under the Directive, the conditions listed in the above bullet-points do not apply to the processing of sensitive data: they are not included in Art. 8(2) of the Directive. The Directive allows States to formulate conditions for the processing of sensitive data in addition to those listed in Article 8(2) – but only (i) for reasons of "substantial public interest" and (ii) provided the State provides "suitable safeguards" for such processing (over and above compliance with the normal rules) in the relevant "national law" (Article 8(4) of the Framework Directive).[150] Most crucially, (iii) these conditions should be specific.[151] Moreover, (iv) such additional conditions for the processing of sensitive data must be notified to the European Commission (Article 8(6) of the Directive).

The conditions in paras. 7(1)(b) and (c) of Schedule 3 do not meet these requirements – quite the contrary: they apply to all processing of sensitive data; they do not relate to any particular "substantial public interest"; they do not contain any special safeguards against undue processing of sensitive data; and, as far as we have been able to ascertain, the United Kingdom has not notified the European Commission of paras. 7(1)(b) and (c) under Article 8(4).[152] At the least, these crucial conditions in the DPA98 which are the basis for most (if not all) of the (sensitive) data sharing arrangements discussed in this study should be extremely restrictively applied, subject to special rules and special safeguards.

---

[149] The UK needs two conditions to cover the two sources of Government authority: Central Government Departments headed by a Minister of the Crown (such as the Home Office) derive their powers not only from statute but also from the Crown, in the form of prerogative powers, and from Common Law, while other departments derive all their powers from statute only. Note that the single criterion in the Directive also covers the additional condition for the processing of non-sensitive data mentioned in the previous footnote.

[150] Article 8(4) reads: "Subject to the provision of suitable safeguards, Member States may, for reasons of substantial public interest, lay down exemptions in addition to those laid down in paragraph 2 either by national law or by decision of the supervisory authority". The Directive also allows for such additional exemptions to be issued by the national data protection authority. This relates to the function of some such authorities (such as the CNIL in France) to issue basic rules for processing: cf. the report on France in Chapter 8. However, the Information Commissioner does not generally fulfil such a role. We will return to the possible actions the Commissioner may wish to take in this respect in Chapter 9.

[151] This is clear from the very terms in which Article 8(4) of the Framework Directive is cast, but also follows from Article 8 ECHR: as discussed under the next heading, these articles interrelate and reinforce each other.

[152] In view of the other defects just mentioned, if the UK were to notify the Commission, the Government would find it difficult to justify these clauses – and they could therefore be challenged by the Commission as incompatible with Art. 8(4). But that is a matter that need not be discussed here: it should suffice to note that the matter cannot be simply remedied by notifying the Commission of these clauses.

In fact, as discussed in the earlier chapters (and confirmed in the DCA's guidance), the Government suggests that institutions wishing to share data should look around for possible statutory provisions[153] which – on the most generous of interpretations – can be said to allow the processing under consideration; as noted earlier, such provisions are referred to as "statutory gateways". As noted in our descriptions in those earlier chapters, some data sharing arrangements appear to rely on the most vaguely-worded and general statutory provisions, such as Section 2 of the Local Government Act 2000.

Reliance on such catch-all provisions cannot be regarded as compatible with Article 8(4) of the Directive, or – and this is perhaps even more important – with Article 8 ECHR, and thus with the HRA. The grave privacy issues raised by the children's databases thus present a significant opportunity for the Commissioner to test the legality of processing on the basis of catch-all provisions. We will return to this issue later.

Before that, we now discuss the only alternative basis for the processing of sensitive data described in this report: the Sensitive Data Order 2000 already mentioned.

The Order is somewhat more compatible with the Framework Directive, in that it sets out a series of reasonably well-defined contexts within which, or purposes for which, sensitive data may be processed.

However, only a few of these can possibly relate to processing covered by this study, i.e.:[154]

- processing of sensitive data for the purposes of the prevention or detection of any unlawful act, where seeking the consent of the data subject to the processing would prejudice those purposes (para.1 of the Order);

- processing of sensitive data to discharge functions involving the provision of services such as confidential counselling and advice, in circumstances where the consent of the data subject is not obtained for certain specified reasons (para.4); and

- processing by the police in the exercise of their common law powers (para.10).

[153] Or prerogative or common law powers. The latter are however, as far as we know, not invoked in relation to the databases and data sharing arrangements examined in this study. Suffice it to note that according to the DCA "[Data sharing on the basis of prerogative or common law powers] is an area where complex legal issues often arise." (DCA guidance section 2, para.9).

[154] The other contexts or purposes covered by the Order are: processing of sensitive data to discharge functions which protect members of the public from certain conduct which may not constitute an unlawful act, such as incompetence or mismanagement (para. 2); disclosures of sensitive data for journalistic, artistic or literary purposes of personal data relating to unlawful acts, dishonesty and incompetence etc. (para. 3); processing of sensitive data in certain insurance or occupational pension scheme contexts (paras. 5 and 6); processing of certain sensitive data for the purpose of monitoring equal treatment (paras. 7 and 9); processing of data on political opinions of individuals by political parties (para. 8); and processing of sensitive data for research purposes – which the Explanatory Note to the Order clarifies as relating to innocuous contexts such as maintaining archives etc. (para. 9).

Para.1 could, in certain circumstances, cover the disclosure of sensitive data by a school or social services to the police (or, in rare circumstances, other agencies). However, it can only be invoked if the disclosure would be "in the substantial public interest" and "must necessarily be carried out without the explicit consent of the data subject being sought so as not to prejudice those purposes." (para.1(1)(a) and (c)). The reference to "the substantial public interest" must, we feel, be read as restricting the application of this provision to cases of serious crime only.[155] This cannot be said to apply to the vast majority of cases covered by this report. In the rare circumstances in which it would apply, we see no problem with the disclosure. It would appear, moreover, that these tests can only be said to be met in an individual case after a careful assessment of that case. The provision therefore does not allow for the routine disclosure of data to the police (or other agencies), as envisaged in the systems described in the earlier chapters of this report. Para.10 could perhaps sometimes be relied upon to allow the disclosure of sensitive data by the police to other agencies, but again this would appear to be fairly marginal to this study.

Processing in relation to "confidential counselling, advice, support or any other service" (para.4 of the Order) could be said to cover several of the arrangements described in this report – albeit far from all of them. However, it is to be noted that this provision too only allows for processing of sensitive data for such purposes if the processing is in "the substantial public interest". This should again be read to mean that there must be a particularly serious reason for any disclosure based on this provision. Some child protection cases will pass the test, but routine child welfare service matters would not appear to be covered. It will be very rare indeed for a situation to arise in which data must be disclosed on a data subject in order to provide a service to that data subject, but in which seeking the consent of the data subject would in itself prejudice the provision of that service.[156]

All in all, the Order therefore has only very limited application to the data sharing arrangements examined in this report.

[155] The reference to such "substantial public interest" appears to be included as lip-service to the requirement of Article 8(4) of the Framework Directive that additional conditions for the processing of sensitive data may only be created when such an interest requires it. However, the Directive would seem to suggest that a particular "substantial public interest" is identified for the additional condition. This is not done in the Order, and to that extent the compatibility of the Order with the Directive is questionable. Our reading of para. 1 gives the term at least some meaning.

[156] Note that this is not the same – and is much narrower – than the situation in which data may have to be disclosed on a data subject in order to provide a service to that data subject, but where the data subject refuses to provide such consent (although that situation is of course also contentious).

Data sharing, the ECHR and the HRA [157]

The European Court of Human Rights (hereafter, in this section, simply "the Court") now clearly recognises that the collection of information on an individual by officials of the state, without consent, constitutes interference with that individual's right to respect for his private life, which is guaranteed by Article 8(1) of the European Convention on Human Rights (ECHR or "the Convention").[158]

According to Article 8(2), such an interference is only allowed provided it:

(i) is "in accordance with the law";

(ii) serves one of the "legitimate aims" set out in this paragraph, i.e.: national security, public safety, the economic well-being of the country, prevention of disorder or crime, protection of health or morals, or the protection of the rights and freedoms of others; and

(iii) is "necessary in a democratic society" for the purpose in question.

Each of these requirements has been elaborately expanded on in the case law of the Court, and some of the matters addressed by it are of crucial importance to this study. Specifically, there is long-established case-law that there are two requirements over and above the requirement that an interference must have some basis in domestic law:

> *Firstly, the law must be adequately accessible: the citizen must be able to have an indication that is adequate in the circumstances of the legal rules applicable to a given case. Secondly, a norm cannot be regarded as 'law' unless it is formulated with sufficient precision to enable the citizen to regulate his conduct: he must be able – if need be with appropriate advice – to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail.* [159]

In addition, the Court has held that any "law" invoked as a basis for an interference with a Convention right must be "compatible with the rule of law, which is expressly mentioned in the preamble to the Convention".[160] The legal rules in question must, in particular, not allow for arbitrariness (the opposite of the rule of law).[161] This in turn

[157] This section draws on "Paper No. 4: The Legal Framework – an analysis of the 'constitutional' European approach to issues of data protection and law enforcement" in: I Brown and D Korff, Privacy & Law Enforcement, study for the Information Commissioner, 2004.
[158] See Amann v Switzerland, Judgment of 7 July 1989.
[159] Sunday Times v the UK, judgment of 26 April 1979, para.49; Silver and Others v the UK, judgment of 25 March 1983, paras. 87 and 88,; repeated many times since.
[160] See, e.g., Malone v the UK, judgment of 2 August 1984, para.67, with reference to Silver and Others v the UK, judgment of 25 March 1983, para.90, and to Golder v the UK, judgment of 21 February 1975, para.34.
[161] Idem.

relates back to the question of how precisely a legal rule is phrased. As the Court observed in a case on secret surveillance powers:

> *The degree of precision required of the "law" in this connection will depend upon the particular subject-matter (...). 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.* [162]

Although this passage refers to secret surveillance measures, the principle is applied generally: legal rules which grant certain authorities the power to interfere with fundamental rights must be formulated with sufficient precision (i) to allow individuals who might be affected to foresee, to a reasonable extent, how the rules will be applied in specific cases, and (ii) to prevent the authorities in question from applying the rules arbitrarily. If authorities are granted discretionary powers, that discretion must be fettered: it must be made clear (if not in the primary rules themselves then at least in other, subsidiary rules or [published!] guidance) when it is appropriate to use the discretionary powers, and when not. In addition, there should be appropriate procedures to ensure that the rules are properly applied, and affected individuals should be able to have recourse to such procedures.[163]

No-one would try to claim that section 2 of the Local Government Act 2000, which allows local authorities to do "anything which they consider is likely to promote or improve [the economic, social or environmental] well-being of their area", allows those authorities to arrest people without other legal authority, or to close down a local newspaper, or indeed to break down someone's front door. Yet this is one of the main provisions on which the authorities seek to base the sharing of sensitive data on children.

The DCA guidance relies on the case of Peck v the United Kingdom as allowing personal data exchanges on the basis of wide statutory provisions in that, in that case, personal data (in the form of a CCTV tape on which the applicant could be identified) was disclosed by a local authority to the press, acting *inter alia* under a broadly-phrased provision similar to Article 2 of the Local Government Act 2000, section 111 of the

[162] Malone judgment, paras. 67–68, references in brackets to other cases etc. omitted.
[163] This procedural aspect of the rights protected by the Convention is increasingly emphasised in the case-law. This builds not only on Article 13 of the Convention (notably the only substantive provision in the ECHR that has not been included in the HRA): the Court increasingly reads such procedural requirements into the substantive articles of the Convention themselves. cf., e.g. for a discussion of the procedural requirements of Article 2 (the right to life), the Council of Europe Human Rights Handbook on Article 2 ECHR, due later in 2006.

Local Government Act 1972.[164] However, it should be noted that this was only one of the legal provisions relied on. The main provision was section 163 of the Criminal Justice and Public Order Act 1994, which specifically allowed local authorities to establish CCTV systems in order, among other matters, "to promote the prevention of crime". The matter was further regulated in some detail in Essex Police Policy Guidelines, which specifically dealt with the question of when CCTV footage could be released to the press.[165] The Court furthermore held that even these combined provisions provided only a sufficient legal basis for the disclosure of *non-identifiable* data without the consent of the data subject. [166]

In other words, the Court accepted (at most) that the above-mentioned provisions, read together, were a sufficient legal basis for the disclosure of non-identifiable data without the consent of the data subject. One cannot conclude from this that those provisions, read together, provide a sufficient basis for the disclosure of personal, i.e. identifiable information – let alone that the broadest provision, section 111 of the 1972 Act, can provide such a basis by itself.

On the contrary, the recent case-law of the Court makes clear (i) that the collecting of personal data (and especially of sensitive data) *ipso facto* constitutes an interference with the data subject's private life, and that the disclosure of such data will constitute a "serious interference" if it can have serious consequences for the data subject, and (ii) that such interferences must be authorised in clear and specific legal rules relating to the particular processing. Furthermore, (iii) the Court has said in a case in which the HIV status of a person had been revealed that:

> *Any State measures compelling disclosure of such information without the consent of the patient and any safeguards designed to secure an effective protection call[s] for the most careful scrutiny on the part of the Court.* [167]

This contrasts with the DCA advice that says:

> *If there are no relevant statutory restrictions it may then be possible for local authorities to share data either internally or externally in reliance on section 111(1) of the Local Government Act 1972 or section 2 of the Local Government Act 2000. The power that is contained in section 2 of the Local Government Act 2000 is of particular relevance as it is designed to ensure that service delivery is coordinated in ways which minimise duplication and maximise effectiveness. Section 2 would permit many types of data sharing partnership between local*

[164] DCA guidance para.3.26, referring to Peck v the UK, European Court of Human Rights judgment of 28 January 2003. Section 111 of the 1972 Act said that "a local authority shall have the power to do anything ... which is calculated to facilitate, or is conducive or incidental to the discharge of any of their functions." For a detailed description of the Peck case, see "Paper No. 4: The Legal Framework – an analysis of the 'constitutional' European approach to issues of data protection and law enforcement" in: I Brown and D Korff (2004) 'Privacy & Law Enforcement, study for the Information Commissioner'.
[165] Peck judgment, para. 37.
[166] For details of the Court's assessment, see paras. 80, 85 and 87 of the judgment.
[167] Idem, para. 78, with reference to Z. v Finland, judgment of 25 February 1997.

> *authorities and others where the proposed data sharing will achieve one of the objects set out in section 2(1) and where there is no statutory prohibition (express or, in very rare cases, implied) restricting the data sharing proposed. Section 2(5) makes it clear that a local authority may do anything for the benefit of a person outside their area if it achieves one of the objects of section 2(1). It should be noted that the Information Commissioner has not expressed a view as to whether section 2 can be relied upon to permit the sharing of council tax data for secondary purposes.* [168]

We recommend that the Commissioner take the opportunity to present his interpretation of the law on this topic, and remind the DCA that European law is also UK law.

Implications of the UN Convention on the Rights of the Child

Finally, it is important to consider the provisions of the UN Convention on the Rights of the Child (hereafter: CRC). Although the CRC has been ratified by the UK, it is not incorporated into domestic law, and is thus not justifiable. However, it is increasingly considered in decisions of the courts in relation to children, and certain articles are particularly germane to the issues under consideration in this report. They reinforce the guarantees under the ECHR/HRA, and should therefore also be taken into account.

Article 5 CRC provides that:

> *States Parties shall respect the responsibilities, rights and duties of parents or, where applicable, the members of the extended family or community as provided for by local custom, legal guardians or other persons legally responsible for the child, to provide, in a manner consistent with the evolving capacities of the child, appropriate direction and guidance in the exercise by the child of the rights recognized in the present Convention.*

The Scottish Commissioner for Children and Young People points out that this also implicitly includes the right of children themselves to seek guidance from their parents.

The importance of the role of parents and family in a child's life is emphasised in all of the human rights instruments, which describe the family as "the fundamental group of society". Decisions about the upbringing, wellbeing and education of children begin as the duty of parents, with the child's contribution to those decisions increasing with maturity, in line with the child's 'evolving capacities' and the Article 12 CRC requirement that:

> *States Parties shall assure to the child who is capable of forming his or her own views the right to express those views freely in all matters affecting the child, the views of the child being given due weight in accordance with the age and maturity of the child.*

[168] DCA guidance para. 3.30.

The fact that a child's views are given increasing weight is not, however, to imply that parents' own views on matters affecting their children can simply be disregarded as irrelevant, or that their over-arching responsibility can be supplanted or ignored where it is convenient to do so. Rather, the process envisaged is one of a gradual shift in the balance of power and responsibility from parents towards their children as each child's experience, maturity and capacity to understand the implications of actions and decisions increases.

By using the expression "evolving capacities", Article 5 makes it plain that the capacity to take decisions does not depend on the age of the child, but on a deeper understanding of his/her personal attributes and development, and on the complexity of the decision that needs to be taken.

Article 16 CRC reinforces Article 8 ECHR, making it abundantly clear that the right to privacy is not merely an adult right that has little relevance for children. It also re-states in almost identical terms Article 12 of the Universal Declaration of Human Rights:

> *1. No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation.*
>
> *2. The child has the right to the protection of the law against such interference or attacks.*

During the passage of the Children Act 2004 through Parliament, the then Minister for Children repeatedly asserted that "child protection is more important than privacy". Because few would argue that where a child is likely to suffer significant harm, the pressing need for action taken in that child's best interests will weigh heavily against privacy considerations, this statement was not challenged. However, it is important to understand what exactly is meant by "protection". In the context of Every Child Matters, it is clear that "protection" does not have the generally accepted meaning derived from the Children Act 1989; rather, as already discussed, it is defined broadly to encompass more general aims such as protecting children from the effects of poverty or from lack of access to services – in other words, 'child welfare'.

It should be borne in mind that, whatever the circumstances, no human right can be disregarded altogether, and nor can one human right be allowed simply to eclipse another, as Anthony Jennings QC makes clear:

> *Any infringement of a Convention right must not destroy the very essence of that right. No public interest can justify the destruction of the essence of a right.* [169]

The powers within section 12 of the Children Act 2004 to establish a universal children's database, and to share information on the basis of statutory duty, were scrutinised by the

[169] Anthony Jennings QC: In the matter of the anti-social behaviour bill, para. 40.
See: http://www.the-childrens-society.org.uk/media/pdf/media/ASB_Legal_Opinion.pdf.

Parliamentary Joint Committee on Human Rights (JCHR) for compatibility with the ECHR. Its final report expressed concern that the powers sought by the Government were not proportionate:

> *We are concerned that, if the justification for information-sharing about children is that it is always proportionate where the purpose is to identify children who need welfare services, there is no meaningful content left to a child's Article 8 right to privacy and confidentiality in their personal information.* [170]

It is in any case wrong to trade privacy against child protection as if the two were inimical.

Privacy is the mechanism by which we define who we are in relation to other people, and as such can be seen as an essential element of child welfare and child protection because it encourages the development of clear personal boundaries. Indeed, many writers on the subject have stressed the vital nature of privacy in self-development and self-definition:

> *Privacy is necessary to the creation of selves out of human beings, since a self is at least in part a human being who regards his existence, his thoughts, his body, his actions as his own.* [171] (Reinman)

> *Changing personal needs and choices about self-revelation are what make privacy such a complex condition, and a matter of personal choice. The importance of that right to choose, both to the individual's self-development and to the exercise of responsible citizenship, makes the claim to privacy a fundamental part of civil liberty in democratic society. If we are 'switched on' without our knowledge or consent, we have lost our rights to decide when and with whom we speak, publish, worship and associate.* [172] (Westin)

> *Privacy is a dynamic, changing process of regulating access to ourselves.* [173] (De Paulo, Wetzel *et al*)

Developing a sense of privacy and autonomy in relation to one's personal life is an integral part of becoming a distinct individual. It is thus important that adults maintain a scrupulous respect for privacy in their dealings with children, in order to reinforce personal boundaries and underline each child's right to say "no" to unwanted intrusion. In this way, the right to privacy directly empowers children to protect themselves.

---

[170] Joint Committee on Human Rights, 19th Report 2003/04.
[171] Reinman, quoted in Introna, Privacy and the Computer: why we need privacy in the information society, 1997
[172] Westin (2003) 'Social and Political Dimensions of Privacy'.
[173] DePaulo, Wetzel *et al*, (2003) Verbal and non-verbal dynamics of privacy.

7.2 Specific Statutory Powers to Share Information

Government is generally aware that data collection and sharing on the basis of general powers and of bullied consent are open to legal objection. There are thus many Acts of Parliament and Statutory Instruments that permit (or are said to permit) data sharing. Here we collate the most important for children's databases. At the end, we will assess these powers in the light of the framework requirements, set out above. Our more general conclusions are set out in section 3.

Youth Justice

Part 3 of The Crime And Disorder Act 1998[174] establishes an entirely new youth justice system.

Section 37 places a duty on "all persons and bodies carrying out functions in relation to the youth justice system" to have regard to the aim of preventing offending by children and young people. This supersedes the requirement of the Children Act 1989 that local authorities should "take reasonable steps… to encourage children within their area not to commit criminal offences".

Section 39 places local authorities under a duty to establish Youth Offending Teams (YOTs) – multi-disciplinary bodies that must include representatives from the police, probation, education health and social services – to co-ordinate youth justice services in the local authority area. Probation, police and health services are placed under a duty to co-operate with YOTs.

Section 41 establishes the Youth Justice Board for England and Wales, a body to oversee youth justice services and to advise the Home Secretary. Local authorities must submit an annual "Youth Justice Plan" to the Board.

Section 115(1) provides that:

> Any person who, apart from this subsection, would not have power to disclose information –
> (a) to a relevant authority; or
> (b) to a person acting on behalf of such an authority,
> shall have power to do so in any case where the disclosure is necessary or expedient for the purposes of any provision of this Act.[175]

A "relevant authority" is defined in this section as a local authority, a health authority, a probation service and the police. Section 219 of the Housing Act 2004[176] amends the section to add to the above list: "a person registered under section 1 of the Housing Act 1996 as a social landlord", and S.I. 2002/2469 adds "a Strategic Health Authority".

[174] Crime and Disorder Act 1998, Part 3: http://www.opsi.gov.uk/acts/acts1998/19980037.htm.
[175] Note the word "expedient", which is clearly more lax than the term "necessary".
[176] Housing Act 2004: http://www.opsi.gov.uk/acts/acts2004/20040034.htm.

Section 115(1) was inserted at Committee Stage in the Lords on government amendment moved by Lord Williams of Mostyn, Minister of State for the Home Office, who explained that:

> *The authority to share information is essential to the partnership approach to crime and disorder which the Bill requires. Much sharing already occurs between agencies under existing statutory and common law powers; for instance, between police, probation service and others. We are concerned that there should be no gaps.* [177]

At Committee Stage in the Commons the Rt Hon Alun Michael MP, Minister of State for the Home Office, stressed that the new clause:

> *…does not give anyone a power to demand disclosure, to override or interfere with any statutory or common law duty of confidence, or the many existing and successful protocols for the sharing of information between, for instance, the police and the probation service; nor does it create a data free-for-all which would have severe implications for civil liberties.* [178]

Education: Connexions

The Learning and Skills Act 2000[179] created Learning and Skills Councils for England and the National Council for Education and Training for Wales, paving the way for the new 'Connexions' service for 13-19-year-olds. Sections 114-122 of the Act provide for widespread information-sharing between agencies, and provide the basis for the "Connexions Card", a smartcard designed as a learning incentive for 16-19-year-olds.

Section 114 of the Act permits the Secretary of State for Education to provide services that "…encourage, enable or assist [...] effective participation by young persons in education or training." A young person is defined as aged 13-19.

Section 117 requires learning establishments to supply any person or body involved in the provision of section 114 services with the name and address of a student and that of his/her parents, together with "[any other] information in the institution's possession about a pupil or student". However, section 117(2) provides that a student over 16, or the parent of an under-16, can forbid a school or college to supply any information about the student other than names and addresses.

Section 119 permits the Secretary of State to supply (any) information, including social security information, to "any civil servant or other person" involved in the provision of

[177] Lords Hansard committee stage 19th March 1998: column 936.
[178] House of Commons Standing Committee B; afternoon 5 May 1998: http://www.publications.parliament.uk/pa/cm199798/cms.
[179] Learning & Skills Act 2000: http://www.opsi.gov.uk/acts/acts2000/20000021.htm.

section 114 services. This allows, e.g. for the provision of information held on Child Benefit or any other social security systems.

Section 120 permits the following to supply information to the Secretary of State or to "any other person or body" involved in the provision of section 114 services:

a) a local authority;
b) a Health Authority;
c) the Learning and Skills Council for England;
d) a chief officer of police;
e) a probation committee;
f) a youth offending team;
g) a Primary Care Trust.

During its passage through parliament, the data protection and privacy implications of the Learning and Skills Act were not debated. It may be that the effects of granting such information-sharing powers to the Secretary of State and to public bodies were not fully appreciated; because of lack of knowledge about developments in information systems and the potential they created for widespread information-sharing.

Education: National Pupil Database

The statutory underpinning for the National Pupil Database is complex because its expansion has been achieved incrementally, both through amendments to the original legislation and via secondary legislation.

The Education Act 1996,[180] section 537 empowered the Secretary of State to make regulations requiring information about any school to be provided by the governing body or, in the case of an independent school, the proprietor. This information could *not* include the name of any pupil. The stated purpose was to measure the efficiency of each school and to "assist parents in choosing schools for their children".

The Education Act 1997,[181] section 20 establishes the framework for the Qualifications and Curriculum Authority and inserts a new section 537A into the Education Act 1996. This empowers Secretary of State to collect "individual performance information" from schools about a pupil's assessments under the National Curriculum, his/her results in public examinations and in the attainment of vocational or other qualifications. In other words, this is personally identifiable information.

The School Standards and Framework Act 1998,[182] schedule 30 para.153 amends s537A to place a duty on schools to supply "individual pupil information" – that is, "information relating to and identifying individual pupils or former pupils" of a school – on request either to the Secretary of State, or to "any prescribed person": that is, any person

[180] Education Act 1996: http://www.opsi.gov.uk/acts/acts1996/1996056.htm.
[181] Education Act 1997: http://www.opsi.gov.uk/acts/acts1997/1997044.htm.
[182] School Standards and Framework Act 1998: http://www.opsi.gov.uk/acts/acts1998/19980031.htm.

prescribed in regulations. The Secretary of State can require information from a prescribed person, or require that it is passed to another prescribed person.

The Secretary of State is empowered to give individual pupil information to a prescribed person or someone "within a prescribed category", and also to an "information collator": that is, "any body which, for the purposes of or in connection with the functions of the Secretary of State relating to education, is responsible for collating or checking information relating to pupils".

An information collator may give (any) individual pupil information to the Secretary of State; to the pupil's school, or to another information collator. In addition, where the Secretary of State so determines, an information collator may pass prescribed individual pupil information to a prescribed person, or to a person within a prescribed category.

Any person holding (any) individual pupil information may provide it to the Secretary of State; to an information collator, or to any prescribed person.

It should be noted that s537A (as amended) says: "no information received under or by virtue of this section shall be published in any form which includes the name of the pupil to whom it relates". The usual meaning of "published" is "made available to the public", and so this is a somewhat weaker provision than a prohibition on "disclosing". The supply of information to a particular group on a particular occasion for a particular reason (but not just to anyone who asks) may not be "publishing" even though the information ceases to be well-guarded.

Various regulations were made under S537A Education Act 1996. The first regulations[183] in 1999 allowed pilots of the new "Pupil Level Annual School Census" (PLASC) to be carried out in England. These were revoked in 2000 by regulations that extended PLASC to all state-maintained schools.[184] These were in turn revoked in 2001 by regulations that increased the range of information collected.[185] A series of amendments – but not revocations – to the 2001 regulations followed, the most recent (2005)[186] requiring more than 40 separate data items, including information about school attendance, and the full postal address of pupils. These regulations are the statutory manifestation of the DfES adding database fields to PLASC as its purposes grew; albeit recoded into English text, since the Parliamentary Draughtsman is not currently prepared to set an XML database schema before the legislature.

In Wales, section 537A was commenced in 2003,[187] initially taking information about post-16 pupils. These regulations were revoked to include all pupils in state-maintained

[183] 1999/989 The Education (Information about Individual Pupils) (England) Regulations 1999.
[184] 2000/3370 Education (Information About Individual Pupils) (England) Regulations 2000.
[185] 2001/4020 Education (Information About Individual Pupils) (England) Regulations 2001.
[186] 2005/3101 The Education (Information About Individual Pupils) (England) (Amendment) Regulations 2005.
[187] 2003/2453 (W.237) The Education (Information About Post-16 Individual Pupils) (Wales) Regulations 2003.

schools,[188] and then a similar incremental increase in the range of information followed over the next two years.[189]

Supply of School Census information to Connexions

Regulations issued in 2002[190] provide that, where a school is not a primary school, a request for information about a pupil under section 537A must indicate whether a young person (or parent) has been consulted to ascertain whether s/he wishes to exercise the right to forbid the supply of information to the Connexions service under section 117(2) of the Learning and Skills Act 2000.

During the passage of the School Standards and Framework Act through parliament, Theresa May MP raised concerns at committee stage about the new powers that the Secretary of State would gain.

While accepting that individual pupil information about exclusions or attendance may be necessary, she said that she was:

> *"concerned that there is no prescription of what information can be passed on to the various bodies. I am particularly concerned about the reference to the information collator. The Secretary of State could require a body that merely provides statistical services, or a market research company, to be contracted to collate information. Such companies would have access to pupil information, which relates not only to exclusions or absences, but gives specific information on individuals."* [191]

The Schools Standards Minister, Stephen Byers MP, replied that the aim was to achieve effective monitoring of under-performance by specific groups, and that:

> *"the matter is technical, and to enable the proper monitoring and evaluation to take place such detail is necessary"* [192]

No further attention was subsequently paid to the amendment in either House.

In 2002 the School Standards Minister, Stephen Timms MP, reiterated in a Parliamentary Written Answer that the collection of pupil names was a technical issue:

---

[188] 2003/3237 (W.317) The Education (Information About Individual Pupils) (Wales) Regulations 2003.
[189] 2005/35(W.2);2005/3238(W.243);2006/30(W.4).
[190] 2002/3112 Education (Information About Individual Pupils) (England) (Amendment) Regulations 2002, para 14.
[191] Committee Reports: Commons Standing Committee A, Schedule 28 School Standards and Framework Bill 3rd March 1998
[192] Committee Reports: Commons Standing Committee A, Schedule 28 School Standards and Framework Bill 3rd March 1998.

> *The Department has no interest in the identity of individual pupils as such, and will be using the database solely for statistical purposes, with only technical staff directly engaged in the data collation process having access to pupil names.* [193]

He set out a list of people who would have access to the database – data subjects, schools and LEAs, and researchers approved by the Secretary of State for Education – and confirmed that:

> *"No disclosures of personal data beyond those listed above are anticipated at this time."*

He went on to say:

> *"The Department does not intend to delete the records of pupils who leave the maintained schools sector, either at age 16 or 18, or before then."*

Children's Services

Part 2 of The Children Act 2004[194] establishes Children's Services in England. Mirror provisions for Wales are contained in Part 3, which is not yet in force. Our emphasis is added below to highlight those areas where definition is not on the face of the Act, but to be made via secondary legislation. The Government has undertaken to submit all regulations governing information-sharing to the parliamentary affirmative resolution procedure.

Section 10 (commenced 1st April 2005)[195] places a duty on "children's services authorities" (defined at section 65 as a county, district or borough council) to make arrangements that promote co-operation between the authority and its "partners", and a corresponding duty on those partners to co-operate. Partners are defined at s.10(4) as any of the following:

- district councils;
- police;
- probation services;
- youth offending teams;
- health authorities, services and primary care trusts;
- Connexions partnerships;
- learning and skills councils.

Section 11(2) (commenced 1st October 2005)[196] provides that all of the above, with the addition of prison governors and any person providing Connexions services, must ensure

[193] Commons Hansard 28 January 2002 (pt 29) column 109-111W.
[194] Children Act 2004: http://www.opsi.gov.uk/acts/acts2004/20040031.htm.
[195] Children Act 2004 (Commencement No.1) Order 2005 SI2005/394.
[196] Ibid.

that "their functions are discharged having regard to the need to safeguard and promote the welfare of children".

Section 12 (commenced on 1st January 2006)[197] empowers the Secretary of State to make regulations under the Children Act 2004 or under section 175 of the Education Act 2002 (see under General Powers, below):

- to require children's services authorities in England to establish and operate databases containing information about children in their area;
- to establish one or more such databases, or arrange for them to be established.

The databases may include any of the following information about a child
:

a) name, address, gender and date of birth;
b) a number identifying him;
c) name and contact details of any person with parental responsibility for him;
d) details of any education being received by him (including the name and contact details of any school/college);
e) name and contact details of any person providing primary health care;
f) name and contact details of any person providing to him services of such description as the Secretary of State may by regulations specify;
g) information as to the existence of any cause for concern in relation to him ;
h) information of such other description, not including medical records or other personal records, as the Secretary of State may by regulations specify.

The Secretary of State may by regulations:

a) specify which items of the above list are to be included in a database;
b) require the following to disclose information: all of the partners; the additional bodies listed above at section 11(2); and any other "person or body of such other description as the Secretary of State may by regulations specify";
c) permit the disclosure of information to: childminders; voluntary organisations involved in providing children's services; the Inland Revenue; registered social landlords; and any other "person or body of such other description as the Secretary of State may by regulations specify".

Regulations may also govern conditions for access to the database, procedures for determining accuracy of the records, disclosure of information, and the length of time for which information can be retained.

Under section 12(11), regulations may provide that all of the above can be done "notwithstanding any rule of common law which prohibits or restricts the disclosure of information".

Anyone operating a database must have regard to the Secretary of State's guidance or directions on its management, technical specifications, security, transfer and comparison

[197] Children Act 2004 (Commencement No. 5) Order 2005 SI2005/3464.

of information between databases, and also to any advice that is given in relation to rights under the Data Protection Act.

General Powers

The following statutes are sometimes cited as justification for sharing information without consent:

Section 175 of the Education Act 2002[198] places a duty on LEAs and governing bodies of maintained schools and further education establishments in England and Wales to make arrangements to carry out their functions with a view to safeguarding and promoting the welfare of children (i.e. under 18-year olds).[199]

It should be noted that this section does not impose any new function upon LEAs or educational establishments; it merely requires that they carry out their existing functions with the welfare of children in mind.

Section 2 of the Local Government Act 2000[200] gives each local authority the power to do anything that promotes the economic, social and environmental well-being of their area. This can be exercised in relation to the whole or part of an area, or any person within the area.

However, section 3 provides that the power "does not enable a local authority to do anything which they are unable to do by virtue of any prohibition, restriction or limitation on their powers which is contained in any enactment (whenever passed or made)".

Furthermore, section 111 of the Local Government Act 1972, which is also sometimes invoked, provides that local authorities are expressly empowered to do anything which is calculated to facilitate, or is conducive or incidental to, the discharge of any of their functions.

Assessment

The statutory provisions and regulations, briefly described above, fail to meet the UK and European requirements adduced in Section 7.1 in several respects:

Sections 37 and 115 of the Crime and Disorder Act, read together, are apparently used to allow data sharing whenever it is "necessary or expedient" to support the functions of a wide range of bodies loosely linked to youth justice, subject only to the requirement that, in this, the aim of "preventing offending by children and young people" is borne in mind. This is excessively vague. It is not even clear that the specific purpose of the disclosure has to be such preventing of offending, let alone in an individual case. As already noted, the term "expedient" furthermore clearly fails to meet the requirement of the DPA98 and

[198] Education Act2002: http://www.opsi.gov.uk/acts/acts2002/20020032.htm.
[199] Commenced 1/6/2004 under SI 2004/1318.
[200] Local Government Act 2000: http://www.opsi.gov.uk/acts/acts2000/20000022.htm.

the HRA of "necessity". The processing in question is said to be covered in more detail in "many protocols", but these are not published or readily available and can be changed at any time without notice to the public. They therefore do not have the quality required for them to be regarded as "law" in terms of the ECHR/HRA – or the DPA98.

The only purpose mentioned in the provision on which the whole Connexions system appears to be based – Section 114 of the Learning and Skills Act – is "[to] encourage, enable or assist [...] effective participation by young persons in education or training." This quite clearly does not cover all the purposes for which Connexions collects and discloses personal data on children.

The provisions relating to the National Pupil Database and School Census information are expressly aimed at monitoring schools or groups of pupils, not individual students. It is quite extraordinary to regard them as authorising the disclosure of data relating to a specific child, for processing by another body in relation to that child, when the disclosing body is expressly said not to be processing the data in such an individualised way.

Section 10 of the Children Act 2004 imposes a duty to cooperate, but without clarifying the purpose(s) of such cooperation. Section 11(2) of that Act (and section 175 of the Education Act 2000) provides the catch-all purpose "safeguarding and promoting the welfare of children", but that is much too vague to be acceptable on its own under the DPA or the ECHR/HRA. Regulations are envisaged but have not yet been issued.

The basic idea seems to be that as long as a body can collect data for any purpose, it can then, thereafter, freely pass those data on to any other bodies for entirely different purposes, as long as those other purposes are specified somewhere else (without too much thought about the specificity with which the purposes are defined). Thus, on this thinking, Connexions can (without consent) pass personal data on children, obtained to "encourage [their] education and training", to YOTs so that the latter can "encourage [them] not to offend"; and the officials maintaining the Pupil Database and School Census information can pass their data (obtained for non-personalised monitoring) to Connexions or YOTs for personalised use – or vice versa in whichever direction – as long as the disclosing body has obtained the data in accordance with the DPA98, and the receiving body performs a function for which the data may be useful.

We believe this approach is fundamentally incompatible with the UK and European legal principles and requirements adduced earlier, and that the promoters of a number of the systems that are the subject of this report are acting ultra vires and/or in violation of the HRA, as well as in violation of the DPA98. In our view, it is not possible to rely on catch-all legislation – such as sections 37 and 115 of the Crime and Disorder Act (read together), section 114 of the Learning and Skills Act, read together with section 11(2) of the Children Act 2004 or section 175 of the Education Act 2002, or section 2 of the Local Government Act – as a basis for sharing sensitive data. Explicit statutory authorisation, or further clear regulation in (published) subsidiary or local instruments, is necessary.

7.3 Summary and Conclusions

Our analysis has shown that the legislative and regulatory framework for the kinds of data collection and sharing described in this study and described in chapters 3 through 6 fails to legitimise the proposed data sharing and processing. There are several problems:

1. Under data protection law, the purposes for which sensitive data are used or shared must be narrowly defined. There are many ways in which the data sharing regime now emerging for children falls short of this. One particularly pervasive example – the shift in meaning of the term "at risk" from "at risk of significant harm or neglect" to "at risk from failing to achieve the government's five targets for children" and "at risk of social exclusion" – could render data protection in respect of children meaningless. It may be tempting to extend the broad data sharing that may be justified in child-protection cases to the much larger class of child-welfare cases, but it is not in accordance with law.

2. A related issue is that under the DPA98 (if applied in accordance with the Framework Directive), no-one (whether adult or child) can give valid consent for processing for a purpose that is too broadly specified. Even on this score alone, the "consent" that is obtained from children and young people for the data sharing described in this report is often not valid.

3. A widespread problem, according to our research, is that "Gillick competence" is being wrongly interpreted and improperly invoked as a basis for obtaining the "consent" of children, between the ages of 12 and 16, for the use and sharing of their data, without parental involvement. However, Gillick made clear that the children's parents must be involved except in those rare cases where the child insists that they not be. Seeking the consent of children or young people without encouraging parental participation can amount, as Lord Fraser put it in Gillick, to a failure by the professional to "discharge his professional responsibilities". In addition, Lord Fraser considered a specific, time-limited situation, in which consent was sought for a clearly-defined purpose (birth control). By contrast, the consent that is sought for data-sharing in the cases examined in this study is often intended to allow a range of practitioners access to a database or other record of information about a child over a long period of time, for a wide range of purposes which may not be at all apparent (to the professional seeking the child's consent, let alone to the child itself) at the time consent is sought. The implications of a single consent to multiple and future acts of data-sharing are far more complex than the situation envisaged in Gillick. This "blanket" consent may, moreover, be taken once only, and the young person may not necessarily be able to know or understand, let alone specify, the people who may (or may not) access the record, nor the circumstances in which they may do so.

4. "Consent" is often obtained by coercion. With regard to many of the databases discussed in this report, practitioners asking children for consent may do so in an environment where children are conditioned to co-operate with the wishes of

adults. This is not conducive to genuinely free choice. In addition, children are often told that providing the information is in their own interest; and that if they fail to consent they may not be able to obtain the full range of "services" they might otherwise receive. These pressures, applied to vulnerable children who may well need help, seriously undermine the validity of any "consent" thus obtained. In those circumstances, professionals must involve and inform parents rather than, as at present, totally excluding them.

5. A person cannot "consent" to the processing of information on anyone else. Processing personal information on parents, siblings and friends of a child, on the purported basis of the "consent" of that child, without either the consent of those other data subjects or some very specific statutory, is quite simply unlawful. This applies a fortiori to the processing of sensitive data.

6. There is a significant opportunity for the Commissioner to clarify an important area of law, which appears to be misunderstood in the legal guidance provided by the DCA. That guidance states that if a statute sets out a public function for a particular public body, data can be disclosed to that body by another body if the data are either specifically needed for the performance of that function by the receiving body, or if they are "reasonably incidental" to that function, unless a specific duty of confidentiality stands in the way of such a disclosure (which can only be assessed in individual cases). More importantly, the guidance allows public bodies to rely on such statutory "gateways" irrespective of the specificity of the provision in question. According to the DCA, open-ended provisions such as section 2 of the Local Government Act 2000 or section 111 of the Local Government Act 1972 suffice for such disclosures and data sharing. However, this guidance is not compatible with the EC Framework Directive on data protection. The guidance is therefore mistaken in terms of EC, and thus (under the ECA) UK law. At the very least, those conditions should be extremely restrictively applied, subject to special rules and special safeguards.

7. A second and alternate ground for challenging the DCA guidance comes from human-rights law directly. The extensive sharing of highly sensitive data on children, described in this report, involves serious interferences with the rights of those children under Article 8 ECHR. Under the Convention, such interferences must be based on legal provisions that are clear, precise, foreseeable in their application and compatible with the rule of law. The same applies to the sharing of data on parents, siblings and friends. Vague and open-ended provisions such as (again) section 2 of the Local Government Act 2000 or section 111 of the Local Government Act 1972 do not meet these requirements and cannot therefore legitimise the data sharing in question. The systems described in chapters 3 to 6 breach the ECHR and, thus, the HRA. Even if data sharing is, at times, (also) based on other, more specific provisions, those could still only be said to allow the interference with the children's rights in question if they contained "effective and adequate safeguards". Such safeguards are largely missing from the current framework.

8. Similar issues are raised under the UN Convention on the Rights of the Child, which in important respects reinforces the protection accorded to children under the ECHR/HRA and which thus helps to clarify the rights in the ECHR/HRA in respect of children. The data sharing arrangements described in this report threaten, and may violate, in particular the provisions in the CRC emphasising the need for respect of the family as a group (Article 5) and the need to respect the right of a child to a private life (Article 16); and the approach to "consent" fails to recognise that children's capacities evolve in relation with their parents, and that parental involvement, rather than simplistic reliance on a child's consent, is therefore often crucial (Articles 5 and 12 read together).

In Chapter 8, we will discuss the regulatory action strategies available to the Information Commissioner to assist in bringing the framework for data sharing more into line with the European and UK legal requirements. Urgent engagement with these issues is needed if serious violations of the law are to be prevented, or stopped. Not only will the arrangements as currently conceived fail to help children and families; they also violate the basic data protection and human rights of the minors and adults involved.

Chapter 8. Analysis and Regulatory Options

There are two sections in this chapter. In the first, we deal with the political, policy and administrative aspects of the children's databases – a guide to the areas of concern with this project. In the second section, we set out a range of regulatory opportunities for the Commissioner to consider.

8.1 The Context of the Children's Database Development

The lead ministry for the children's databases is DfES, which operates in a public-sector IT environment with which the Commissioner will be broadly familiar. The policy drivers start with wide-ranging goals at the national level (ending child poverty, reducing social exclusion, being tough of the causes of crime) and work down through a series of initiatives (such as Communities that Care) that are broadly speaking the purview of junior ministers, via a civil service apparatus of policy, architecture and systems delivery.

There is always a risk of a disconnect between these levels, but this disconnect appears to be particularly severe at DfES. For example, officials to whom we talked at the architecture level were unaware of policy issues (such as Gillick) in the layer above them, and ignorant of the details of the systems being developed by the layer below. Technical people, from the architecture layer downwards, appear to assume that data protection concerns 'have been taken care of'. These concerns do not even seem to be well embedded at the policy layer, but off to the side in the legal unit. This makes it rather difficult for good data protection practice to be embedded in systems design. The risk is that systems will be developed defensively, with access to more information than actually needed for a specific purpose, and then protected after the fact by introducing new regulation. System designers do seem to fear that they might be blamed for failing to collect some item of data that might have prevented some future tragedy and this encourages over-inclusiveness.

Observers of public-sector computing will already be aware of this danger. In the early 1990s, when plans were being laid in the NHS for what has now become the NPfIT, the team took strategic decisions based on the assumption that centralising all medical records on a single server farm was the best way to proceed. These decisions have had unfortunate effects, both in cash and privacy terms, and in creating tensions in relationships between the Department and the professions. The DfES team is, like the NHS team then, a recent creation; it is well known that teams take time to acquire competence.

A further parallel with health can be seen in the negative reaction of social work professionals to the Children Act; they were concerned that information sharing would lead to other agencies passing their problems over to already-overstretched services. This echoed medical objections to NHS computerisation in the mid-1990s. We do not want to labour the parallels between health systems and social care systems, but they must be

borne in mind. There is a positive difference: while DoH goals are firmly entrenched after more than a decade of struggling with professional objections, DfES is just starting out. Officials to whom we talked said they would welcome a constructive engagement with the Information Commissioner in order to avoid design errors that could lead to problems later.

A Policy Caveat

We are concerned that the network of children's databases lacks a clear policy justification. On being first elected in 1997, the Government started to follow an evidence-based policy for primary crime prevention and delinquency reduction through initiatives such as Communities that Care and Sure Start. However, it appears to have been unable to make these policies work: the evaluations of the Sure Start pilots are not positive, and CtC appears to have languished. Rather than finding out what was wrong with the implementation, ministers appear to have fallen back on generalities ("a mixture of population-based and targeted strategies") and placed their faith in technology. The database initiative now appears to be driven by the e-government agenda rather than by child protection, child welfare, or even realistic crime-reduction goals.

The best explanation we have heard for the failure of Sure Start was that the various pilots lost their focus as they acquired subprojects reflecting assorted local and personal interests; if this is correct, then the loss of focus at the centre is serious. If no effective interventions are available then it is hard to see the justification for any privacy intrusion. There might be some justification for data collection if YIPs worked; but they do not seem to work well (and even then, the selection of children for a YIP would have to involve professional judgement rather than automatic scoring if it were to be legal – the database could at most help inform this judgement).

The Information Commissioner might of course take the view that a concern at this level is not a matter for data protection law, but for Parliament.

Confusion Within and Between Services

The next set of concerns focus on the confusion of goals, reasoning, guidance and even terminology between – and within – departments. This is a standing problem with social care, as social workers and allied professions still do not have an agreed professional vocabulary. There is one particular point of confusion, however, that appears to circumvent at least the spirit of data protection law, and which the Commissioner should help to resolve.

This point is that "child protection" and "child welfare" are not the same thing. Child protection refers to protecting children from a real risk of significant harm from abuse or neglect, usually from their parent or carer; there has never been any problem in the UK (or elsewhere) with the proposition that confidentiality can be broken on child-protection grounds. This has long been an integral part of the daily operations of social workers, doctors, teachers, the police, and data-protection officers. Child welfare is a much broader category, referring to children who are poor, or unhappy, or living in

unsatisfactory neighbourhoods, or at risk in some other way of not growing up into happy adults with a reasonable chance to fulfil their potential.

While child protection deals with a small number of children, with around 50,000 children on the child protection register in England child welfare concerns may exist for 3 to 4 million. The effect of the Every Child Matters agenda is to extend social care from protection to welfare, because of the quite reasonable argument that in the past, social care has been too reactive to be effective; that parents struggling with multiple problems ask for help but do not receive it until they snap and hit their child. This is thoroughly sensible. However, the data-protection attitudes thought by some to be appropriate in child protection (namely, that data protection concerns are overridden by immediate concern to protect human life) appear to be percolating from protection into welfare. The Information Commissioner must, we believe, challenge this. The further extension into (and blurring of boundaries with) crime prevention complicates matters still further.

The core subjects of this report are thus the balance between child welfare and privacy, and between crime prevention and privacy. On the welfare side, there are many circumstances in which privacy should prevail in the interests of the child, and in which rational and caring parents will therefore refuse information sharing. For example, the stigmatising effects of social-work intervention are real, and the services offered to low-priority families are so meagre, that it may often be rational for parents struggling with minor problems to simply soldier on. On the crime-reduction side, there are other issues relating to proportionality. We cannot believe that a police force is justified in sharing information without consent about a nine-month-old baby on the grounds that it might grow up to be a villain. Measures that may be justified in the face of specific and identified threats lose their justification when they become statistically-based measures against subpopulations.

As in medicine, there are also legitimate professional concerns. Confidentiality has significant therapeutic value in child welfare. There is a substantial body of evidence showing that children are less likely to seek help if there is no confidential service available. They want to be able not just to discuss their problems, but to retain some control of what is done. Most victims of child abuse do not seek help from the child protection services.[201, 202, 203] Childline, however, a phone helpline that does offer confidentiality, has proven to be far more acceptable. It has long been known that advice on sexual matters is in general much more valued and effective if confidential; and research shows this to be also the case where the patients are children.[204]

[201] I Butler, H Williamson (1994) Children Speak: children, trauma, and social work. Harlow, Longman.
[202] P Cawson *et al* (2000) Child maltreatment in the United Kingdom: A study of the prevalence of child abuse and neglect. London, NSPCC.
[203] C Wattam (1999) 'Confidentiality and the social organisation of telling', in N Parton, C Wattam (eds.) Child sexual abuse: responding to the experiences of children.. Chichester, Wiley.
[204] A Weyman, C Davey (2004) 'The right to confidentiality: young people's access to sexual health services'. Childright, 211, pp.6–7.

Administrative Consistency

Our third headline point is the well-established principle in law that sensitive information cannot be shared using catch-all provisions such as the Local Government Act 1972; such provisions merely empower an authority to spend money on a project without thereby acting ultra vires. They do not allow data controllers to override or ignore either data protection law or a common-law duty of confidence. For that, explicit regulation is in general required.

Here, the operators of the various children's databases vary quite widely in the quality of their regulatory compliance. The systems used in schools, such as the National Pupil Database, have had regulations made under appropriate Acts, and the DfES appears to be well aware of the need to promulgate suitable regulations for IS and ICS in due course. (Whether the system designs and the eventual regulations will fall foul of human-rights law and European law is of course a quite different matter.)

Other departments appear to be less punctilious: we have been unable, for example, to find the regulations, rules or guidance documents governing the majority of the systems used in youth justice and probation. The Youth Justice Board website places some emphasis on the crime-prevention exemptions in Section 29 of the Data Protection Act 1998, while their published guidance[205] also refers to an order made under "paragraph 10 of schedule 3" (presumably of the Data Protection Act) and cites the "Background Legislation" paper on their website – which turns out to be silent. The order is in fact The Data Protection (Processing of Sensitive Personal Data) Order 2000 SI no 417. However, it should not take specialist knowledge to find this. Someone involved in a privacy case, such as a family solicitor, ought to be able to find out whether someone who compromised privacy acted lawfully or not; the same holds even more strongly for a professional such as a doctor or social worker, confronted with a dilemma about whether or not to share information.

To be fair, the YJB guidance does acknowledge at one point that, because of the voluntary nature of preventive support and intervention, "any need to share information without consent is expected to be minimal and is likely to be restricted to the early identification stage of those children and young people who are at risk". However, the general tenor of their guidance is that consent is rarely needed. DfES has explicit and findable regulation, but its guidance contains vague and threatening phrases such as "it may be dangerous not to share information".

The prevailing message is that sharing information is necessary to improve outcomes for children, and this colours the way in which families are asked to give consent. There seems no awareness that people might have rational, defensible reasons for disagreeing with the government's message in relation to their own family on a particular issue. This bias is illustrated by the continual references to "obtaining consent to sharing information" rather than "seeking the views of families on whether to share information".

[205] 'Sharing Personal and Sensitive Personal Information on Children and Young People at Risk of Offending – A Practical Guide', Youth Justice Board 2005

It is also illustrated by the requirement that practitioners need to "understand how to present genuine choices to young people and how to obtain consent to sharing information".[206]

There is a very strong case for greater clarity and consistency across government. The DfES, the Home Office, the Social Exclusion Unit and the Department of Health (to name only four) have significantly different approaches. The definitions are also ambiguous and confusing; 'at risk' sometimes means 'of serious abuse' and sometimes 'of social exclusion', leading to lack of clarity and thereby putting the projects at serious risk of unjustifiable function creep.

A particular case of the above is the attitude to parents. Some government documents strongly endorse the importance of their role in child rearing, e.g. "Parents are the best judges of their family's needs",[207] while others assume it is right to override their views whenever these are in tension with professional practice. A third viewpoint is that parents' rights may be overridden for mere administrative convenience.

Many of the greatest areas of disagreement concern consent. Taken as a whole, the advice from different government departments on consent is incoherent, and likely to cause confusion to professionals, parents and children alike. The need for consent to be voluntary is frequently misunderstood, with some documents recommending asking for consent as a condition of providing a service; the authors appear unaware that coerced consent has little legal effect (and may have the reverse effect of that intended). The biggest single consent issue, however, is the practice of asking children to consent to data sharing without consulting their parents. The settled law of the land – Gillick, confirmed by Axon – is that parents should be consulted unless the child disagrees and is mature enough to understand the consequences of that decision. It is widely misinterpreted as carte blanche to obtain (perhaps coercive) consent from children without informing their parents. A key concern here is how Section 12 of the Children Act 2004 will be regulated. This contains the potential for making information sharing a statutory responsibility, and therefore compatible with the Data Protection Act 1998.

It has often been noted that professionals are unsure of, or mistaken about, their duties/powers to share information without consent. It is implicated as a significant cause in some child death inquiries. The guidance collected in relation to the different databases in social care, education, and youth justice varies considerably and this will lead to confusion as professionals from these different domains work together in relation to a particular family. For safety reasons, government guidance on information sharing needs to be clear and unambiguous; it should not use hints and subliminal pressure to signal that breaching confidentiality is the default; it must be balanced, showing respect for individuals' wishes to have confidentiality as well as having regard to the services' convenience; and it must understand its own limits. It should not try to transgress on areas of professional expertise and ethics. Recognition must also be given to the vulnerability of parents due to the power imbalance with professionals. Many are scared

[206] In 'The common core of knowledge and skills for the childcare workforce', DfES, 2005, p.8.
[207] para 1.6 Choice for parents, the best start for children: a ten year strategy for childcare, DfES, 2004

of being judged as bad parents if they disagree in any way with professionals' views. Research has shown how difficult parents find it to challenge professionals even on a factual error.[208]

Costs and Benefits of Information Sharing

The YJB guidance assumes that since early-onset hyperactivity has apparently been statistically linked to an increased likelihood of criminal behaviour later in life, doctors should automatically notify police, social workers and schools of such diagnoses. This is justified (as indeed is information sharing in general) with the observation that different agencies hold the different risk factors on a target child.

However, from the viewpoint of medical ethics, it is unlikely that such a rationale would be accepted. Doctors automatically share with the DH information on notifiable diseases such as typhoid and leprosy – diseases whose communication could cause death or grave harm to others, and which are treatable. Early-onset hyperactivity is not a direct cause of anti-social behaviour disorder later in life, as far as anyone knows, but merely one of a large number of associated factors. There is then also the question of treatment. Even if antisocial personality disorder is in fact a single disease (which is disputed), we don't know how to treat it. The scarcity of effective therapies distinguishes social work from medicine. In the relative absence of an ability to help, the principle of 'First do no harm' applies with even greater force to social work than it does to medicine. In other words, the balance should be even more strongly in favour of confidentiality than it is in medicine.

In child welfare, data sharing also seems to carry elevated agency risks. A US study compared 12 counties that had child welfare coordination teams with 12 that did not. It was found that inter-organizational service coordination in public children's services systems was negatively associated with service quality, a finding that the authors attributed to decreased individual accountability for care.[209] There was no association with children's outcomes. Similarly, in the related context of children's mental health care, systems integration has been associated with some improvements in access and satisfaction, but has not improved children's clinical outcomes.[210, 211]

The benefits of information sharing to child welfare strike us as frequently overstated, *inter alia* because of the long and tenuous causal chain between data sharing and improved outcomes. A practitioner who identifies a need may share information in order to help herself or others assess that need more accurately; if this does in fact happen then

[208] B Corby, M Millar, L Young (1996) 'Parental participation in child protection work: rethinking the rhetoric.' British Journal of Social Work, 26, pp.475-492

[209] C Glisson, A Hemmelgarn (1998) 'The effects of organizational climate and interorganzational coordination on the quality and outcomes of children's service systems'. Child Abuse and Neglect, 22(5) pp.401-421.

[210] L Bickman, K Noser W Summerfelt (1999) 'The long-term effects of a system of care on children and adolescents'. The Journal of Behavioural Health Services and Research. 26(2) pp.185-202.

[211] L Bickman, W Summerfelt, K Noser (1997) 'Comparative outcomes of emotionally disturbed children and adolescents in a system of services and usual care'. Pyschiatric Services, 48, pp.1543-1548.

the type of help needed may be determined more accurately; and then, if the resources are available and the help is provided in a timely manner, the child's outcome may be improved. But problems arise at each step. There is an absence of evidence that sharing improves outcomes (and actual evidence of harm, as noted above); there is a shortage of resources, to the extent that teenagers attempting suicide have at best a 50% chance of getting counselling (and less in some areas); there is at best weak evidence of practitioners' ability to provide effective help, with inconsistency in service quality across the country and a lack of reliable evidence about what works best in social care.[212]

Child protection (as opposed to welfare) provides an example of where collecting and sharing information has been part of good practice for decades, but the experience even in this area of work illustrates the complexity of the process. There is much more to information sharing than just removing legal obstacles and improving sharing procedures. In children's welfare, much of the information is ambiguous, so open to rival interpretations. The poor reliability and validity of much of the sensitive data is well known: research has consistently found a low level of inter-rater agreement between professionals on identifying need or judging the quality of parenting.[213, 214] The significance of an item as a warning sign is not self-evident.

The negative effects of stigmatisation must also be considered; it is quite possible to do harm by collecting and disseminating information. The simplest 'dark scenario' is that an innocent child caught up in a police enquiry is treated as a suspect, and alienated as a result. There is a much more serious systemic concern: that by collecting information indicative of, or correlated with, future delinquency, and doing so on a huge scale, the database systems are creating the basis for a new, high-tech form of discrimination. If the offence of 'Driving While Black' is replaced over time with 'Driving while having more than 80 points on ICS', then the system will fall foul of data protection principles in a number of ways. Were the data relevant, and not excessive? Were they processed fairly and not held for longer than necessary? If (as seems likely) the answer to one or more of these questions is 'yes', then is the Section 29 law-enforcement exemption an adequate get-out-of-jail card for the data controllers? We think not.

A further sanity check is to translate child-welfare claims to an adult context and ask whether they make sense. For example, if a town had a problem on Saturday nights with drunken fighting, then the authorities might reason that fighting is associated with alcohol intake, with living in poor housing and with being in a community where hitting people is a badge of honour. The logical conclusion would be forcible collection of data on alcohol consumption and its correlation by postcode; obtaining lists of suspects from pub landlords and police; and then a program of alcohol-awareness programs, anger-management classes and so on which all men scoring over a certain level would be required to attend regardless of whether they had ever been in a fight. Examples like this

[212] Department of Health (2000} 'A Quality Strategy for Social Care'
[213] B Daniel (2000) 'Judgements about parenting – what do social workers think they are doing?' Child Abuse Review, 9, pp.91-107
[214] M Little (1999) 'Prevention and early intervention with children in need', Children and Society, 13, pp.304-316.

make it clear that a distinction must be drawn between preventing crime where there is a specific, identified threat, and generally discriminating against groups of people in the name of general prevention.

Finally, the balance between child welfare and privacy must be considered not just as a matter of law and administrative convenience but of humanity – at stake is not just therapeutic effectiveness but children's rights. People regulate their relationships by choosing what level of intimacy they wish to share, and with whom. Promoting respect for children's personal boundaries is thus an important ingredient in empowering them to resist unwelcome intrusions into their private space.

8.2 Possible Regulatory Action Strategies

This leads us to suggest three possible regulatory action strategies for the Information Commissioner.

The first strategy requires minimal action and entails the Commissioner simply following previous UK practice – issuing enforcement notices for the most serious problems but generally hoping to encourage departments to issue regulations and guidance that formalise existing and planned practices.

In the second possible strategy, the Commissioner seeks to engage government and the public in a debate about the right balance between privacy and child welfare, and to influence not just the shape of regulation but the design of the next generation of systems.

In the third possible strategy, the Commissioner would take an even more active role by challenging a number of existing UK practices which would not be legal in other European countries. The Commissioner could also challenge the Government to provide evidence of benefit to balance the harm done by privacy intrusions, and rule against such intrusions where evidence could not be produced.

In the next three sections, we outline how each of these strategies in turn might develop.

#1 Minimal Strategy

Even if child welfare is not considered to be suitable ground on which to develop data protection vigorously, and the Commissioner decided on a low-key strategy focussed on educating data subjects and controllers, there are nonetheless a number of clear breaches of the law – and ignoring these could undermine the credibility of data-protection law and of the ICO.

1. First, some departments and local governments do not understand that general catch-all powers are insufficient to compel the sharing of sensitive information. Those who lag behind in this regard need to be brought up to speed with the best existing practice (such as DfES). Even so, the best practice needs to be improved

– ‘trailblazer’ projects are at present often operated under general powers and are thus unlawful in the absence of proper consent.
2. Specific abuses include the abuse of ethnicity data in schools and the use of discretionary powers to override refusal of consent to information-sharing.
3. The previous Information Commissioner objected to the use of unique numbering systems in schools. This has crept back in, and action is required.
4. Families are often unaware that they can opt out of much information sharing in respect of social care, education and health systems. The Commissioner could consider providing clear guidance on this. More generally, he could work with the relevant professional bodies to develop consistent guidance that is accessible to professionals, parents and children.
5. Further guidance is required for system developers on automatic processing. Many system builders seem to be unaware that while automatic processing is fine for routine matters such as repeat prescriptions, and even to point out possible cases of concern to a social work department, there must be a human (and indeed a professional) decision to take an action that could significantly affect the data subject, such as issuing a multi-agency alert.
6. Agencies might also usefully be reminded that they should not use the Data Protection Act 1998 as a mere excuse for inaction, for example where a secondary school wants cohort data from local primary schools and this can easily be passed on in statistical form.
7. Finally, the most important area in which the Commissioner should educate data controllers is in the area of consent. There is very widespread misunderstanding of the law on this point, which is not acceptable given that the law established in the Gillick case was recently confirmed in Axon. These judgments are commonly misrepresented by the operators of systems holding information on children as saying that once a child has passed the age of thirteen, there is no need to involve parents – the child can be asked for consent. This is not what the courts said. When obtaining consent from minors, the parents should normally be involved. If the child insists, and is judged capable of understanding the consequences of its decision, then the parents may exceptionally be excluded from the consent process. However, in the great majority of cases the child is likely to agree to parental involvement (bearing in mind that this report is about child welfare cases, not child abuse cases). Indeed, by unlawfully depriving parents of a say in matters of consent, the data controllers are often acting against the child’s interests. This is particularly the case where (as unfortunately seems common) there is an element of coercion in the consent. The Commissioner should make clear, as the law does, that parents must be involved in consent decisions unless there are compelling reasons to the contrary (such as the refusal of a Gillick-competent data subject) – and that in any case coerced consent has no effect in law.

Level #2 Moderate Strategy

Although a *de minimis* regulatory strategy would bring some benefits, we believe that the Commissioner could be more ambitious. The network of children’s databases is not yet built, and a number of crucial design and regulatory decisions appear to be pending. The most significant of these is the ICS, which may in time play the same role in child social

care as the NHS CRS was supposed to play in the NHS. It would be a valuable public service if the Commissioner could help the DfES avoid the problems that have plagued that system over the past ten years – many of which had their roots in privacy issues for patients (and related professional-autonomy issues for clinical staff) undermining professional acceptance.

Under this option, the Commissioner would become more closely engaged with Departments to bring everyone up to the standards of the best, and to educate them about the need to comply with European law. He would challenge the balance of benefit and harm in proposed system designs, and not accept one-sided accounting. He would audit systems as they are used, rather than at the level of specification. In particular we would add the following recommendations to those of the section above.

1. The Commissioner could engage vigorously in the design and regulation of ICS and eCAF. For example, much of the information to be held therein is 'intelligence' rather than 'evidence', and this raises a whole slew of issues familiar from police systems. The best practice there should be adopted here too: information should be tagged to note its source and reliability, so that a child does not end up stigmatised for life because of a chance (or malicious) comment. In any case, without such measures, the quality of data held in the system is likely to become so poor that little reliance could be placed on it. When assessing plans for ICS, the Commissioner should have regard to how the current users of precursor systems such as Connexions actually behave, rather than just to the theory.
2. The Commissioner should also get involved in the regulation of Section 12 of the Children Act 2004.
3. The Commissioner should push for much clearer rights to opt out of data sharing systems. At the very least, all parents (and not just celebrities) should have the right to opt out of IS, unless there are child-protection (not just child-welfare) concerns. An opt-in design would be even better.
4. The Commissioner should review the sensitivity of meta-data. The presence of an LEA code rather than a school code on NPD, for example, reveals that a child was being considered for care at the age of four. 'Sensitive services' should not just be limited to drug treatment, mental health and genito-urinary medicine services but should also include social services. If a child is known to social workers, the family often wants this to be confidential because of a quite rational worry that teachers might have lower expectations. Some hard design decisions here are getting fudged.
5. The Commissioner should take a much harder line on stigmatisation and discrimination. In Germany, for example, kindergarten data cannot be passed to the primary school. Sharing data must not just be a default – parties wishing to share must be under an onus to show real advantage. He should educate both policymakers and the public about the real risks posed by discrimination, and point out that uncontrolled sharing of stigmatising data is inconsistent with the social inclusion agenda.
6. The Commissioner should also see (and promote) this strategy in a broader context: other social care systems such as mental health and elder care will

follow, and if children's systems are not developed properly there will be further problems later.

7. A really important aspect of this more vigorous strategy is once more to educate policymakers and system builders on the law. As well as Gillick, compelled consent and catch-all powers, we recommend an education programme on how the Data Protection Act must be interpreted, in the light of European law and the Human Rights Act, and on the growing gap between Britain and the rest if Europe on data protection practice (see Chapter 7 and the Appendix). We also suggest that the Commissioner push for the regulations passed to facilitate data-sharing in public-sector systems to be accessible, in the sense that they should be comprehensible to a family solicitor as well as being sufficiently well-indexed to be found online. (Departments should do this anyway; the Commissioner might usefully promise that his website will do it for them if they don't do it properly themselves.)

The overriding theme of this strategy is to work actively to minimise harm. Rather than confronting ministers directly over policy initiatives, the Commissioner works to entrench and clarify the framework of law within which he operates, and to bring home to Departments that ignoring it or attempting to circumvent it carries costs.

Level #3 Vigorous Strategy

In the long run, departments may build systems that infringe human rights and European law, and attempt to deal with the data-protection objections by legislation or regulation. In the field of school systems, for example, the NPD has expanded from its initial statistical purposes to become a nationwide surveillance system. The organisational pressures that lead to such mission creep are well enough known and need not be discussed further here. The problem is what to do about them, especially as the DfES has been fairly punctilious (by comparison with other departments) about taking powers that, at least superficially, legitimise these operations.

Ultimately we suspect that data protection cannot achieve its mature role within the governance of the UK until the Commissioner has an effective means of challenging regulations on privacy grounds. This is already the case in many European countries; for example, in France, the CNIL is consulted on relevant regulation. Perhaps an interesting analogy might be drawn with CESG, the department responsible for information security within government. Its direct influence over departmental security officers enables it to enforce rules on matters from clearances and training to the handling of cryptographic key material. The Information Commissioner's operations would be similarly strengthened if departmental data protection officers had a dotted reporting line to the ICO, so that they could be properly trained and brought within the data-protection community – rather than (as it seems to us) seeing their function as protecting their department from the Commissioner.

In a country like Britain with a gradualist constitutional tradition, this may have to be built in stages as the opportunity presents. One interesting aspect of the children's

databases is that they provide a number of opportunities for the Commissioner to make his position clear from the outset.

There are a number of regulations whose proportionality is open to challenge, including those for the NPD and IS. IS in particular can be attacked as a response to a non-existent problem. In the absence of evidence of any necessity for intervention, and of the efficacy of the available interventions, a strong case could be made in human-rights law that such systems are not justifiable, and must not be operated – except with full informed consent, or in cases of an overriding child protection (as opposed to child welfare). This is reinforced by the likelihood of stigmatisation causing actual harm, as discussed above.

The direct regulatory goal here would include limiting the use of IS references to protection cases, as opposed to welfare cases. The public emphasis during the campaign would be the enormous increase in the quantity of data that will be recorded about children who are not believed to be at risk, and the various hazards (to safety as well as privacy) that follow. Such a goal would have strong support in European law (which is also British law) and practice.

A second option, given that intervention is likely to be resisted less fiercely in the case of systems that have not yet been built, would be to tackle ICS and cut back its scope from child welfare cases to child protection cases. This would have perhaps even stronger support in European law and practice.

A core part of the argument here would be that while information sharing can be useful in child protection, its utility in child welfare is very much open to challenge and thus the proposed ICS system amounts to a large-scale experiment. A data protection analysis must be informed by ethical considerations; there should first be pilots followed by research that asks 'for what problems are we providing an effective solution?' The pilots must also study the risk of harm, under a number of headings. These include:

1. the loss of therapeutic value and of public trust: there is evidence from many studies, including a forthcoming study by the Children's Commissioner, that children value confidentiality and without it will be reluctant to talk about their problems;

2. the evidence from effectiveness research of preventive programmes causing worse outcomes (e.g. USA delinquency prevention programmes that led to higher rates of delinquency). There are also the negative evaluations of Sure Start. With this history, there is a moral duty to check for harm before national implementation;

3. the risk of creating a new form of discrimination. ASSET and ONSET try to predict who will be re-offend or become delinquent, and their scientific basis is at best weak, so the rate of false positives is very high and children thus stigmatised may suffer real harm;

4. the risk of reducing still further professionals' contact time with families with a consequent effect on the quality of working relationships. The time required to enter and access data on computers is dramatically changing work patterns, and recent research found front line workers were on average now reduced to five hours of contact time with families per week;

5. the risk of decreasing operational effectiveness by spreading responsibility and evading both personal and institutional liability, as described in the reported US studies;

6. the fact that information sharing will cause some harm directly. A woeful example of this is the recent case of a nine-year old unlawfully taken into care following the misunderstanding by social workers of some medical information.[215] There are two types of error in child-protection cases; missed alarms (Climbié) and false alarms (this case, Orkney, and others). The trade-off between false alarms and missed alarms is well-studied in fields as diverse as electronic warfare and biometrics; increasing the volume of available data while decreasing its average quality can simultaneously make both error rates worse.[216]

A third option is to focus tightly on the stigmatisation issue, and insist that systems not be used to aggregate data that will be used to create new, high-tech forms of discrimination against children and young persons who have high scores of negative factors, but who may in fact be upright citizens who obey the law despite their disadvantages. Particular attention might be paid to all systems that store data on ethnicity or on postcodes. Any discrimination system that has access to ethnicity data is clearly suspect (early versions of some systems appeared disposed to focus on travellers' children, but we are assured that this has now been rectified). Access to postcodes gives access to social class, and also in many places to a proxy for ethnicity. The Commissioner should thus be justified in demanding full access to the specifications of any system that uses such data and subjecting it to a rigorous audit. A campaign on this topic might chime well with the government's social inclusion agenda.

Finally, a fourth option (independent of the others) would be for the Commissioner to start to offer opinions on the extent to which proposed laws and regulations comply with the data-protection aspects of European law. The present system whereby ministers certify human-rights compliance is unsatisfactory; where a minister is poorly advised, correct advice should be offered sooner rather than later. Of course, were ministers to consult the Commissioner, as in France, the incidence of disagreement would be much reduced. However, it does not help the public (from the point of view of foreseeability) if the Commissioner's objections only become apparent after a specific complaint.

---

[215] Council must pay £500,000 for wrongly taking girl into care, The Guardian, 17 March 2006, at http://www.guardian.co.uk/uk_news/story/0,,1732849,00.html; legal reference is Re X: Emergency Protection Orders [2006] EWHC 510 (Fam)

[216] Biometric decision landscapes, J Daugman, Cambridge University Computer Laboratory Technical Report no. 482, at http://www.cl.cam.ac.uk/TechReports/UCAM-CL-TR-482.pdf

Conclusion

This is a critical point at the evolution of data protection law and practice in the UK. Britain has paid less attention to privacy than our continental partners; the weak implementation of European data-protection law and the poor resourcing of the Information Commissioner's office are familiar enough complaints. At the same time, a number of centralising initiatives (from the NHS Care Records Service to the ID cards project) have combined to raise public disquiet about privacy.

At this juncture, the arrival of IS and the proposed construction of ICS, together with the proliferation of education and youth-justice systems, present a serious regulatory challenge. Because of the scope and complexity of the proposed collection of sensitive data, there is no doubt that data protection law (and human-rights law) will be broken. Not all of these breaches will be within the Commissioner's remit; but some of them certainly will be.

There is thus an opportunity for the Information Commissioner to develop his office in the direction of the better-entrenched and better-resourced authorities to be found on the continent. It is important that he does so. The children's database systems will shortly be followed by other social-care systems, notably for older people and for the mentally ill. Data collection under the rubric of social care will leave few families in Britain untouched. Ultimately, if illegal systems are built, they will be challenged in the courts. If the Commissioner prevents that by regulatory action now, he may irritate the system owners in the short run – but will save much more anguish and expense later.

Appendix. Regulation Elsewhere in Europe

Data protection law is ultimately a European matter, being based in EC Directives and the ECHR and open to appeal in the European Court of Justice and the European Court of Human Rights. It therefore makes sense to study how other countries in Europe deal with the tensions between child protection and children's rights; if the UK were to stray too far from the European norm then it would be exposed to action, whether legal or legislative, to bring it back into line.

(A) The Legal and Regulatory Framework in Germany [217]

Germany can be an interesting reference point in comparative studies of European data protection law, as (with France) it tends to lead other countries in the development of this law.

A.1 Background

In order to understand the German legal and regulatory framework, two matters need to be noted. First of all, the decentralised, federal nature of the country: many matters of relevance to our study are traditionally dealt with at the local, regional or (at most) at state (*landes*-) level, rather than at the federal (*bundes*-) level. Education, social welfare and policing are local or state matters, with the federation playing merely a coordinating role or acting in special matters (e.g., on police matters, through the federal police bureau, the *Bundeskriminalamt* or BKA). The relevant (state) laws moreover generally leave room for professional discretion on the part of (e.g.) teachers and social workers, within an agreed legal framework, as further discussed in section 3, below.

Data protection, at least in the public sector, is also largely a matter for the states: the data protection rules relating to the kinds of activity just mentioned are laid down at the state level, in *Landesdatenschutzgesetze*. There are therefore, in Germany, no less than 16 general data protection laws (the Federal Law and one for each of the 15 *Länder*). In addition, there are numerous other laws that either deal with data protection in a specific context, or that otherwise contain data protection rules. At state level, this includes laws on schools and social work. Supervision and enforcement is similarly spread over a range of different authorities including a data protection commissioner for each *Land* and one for the Federation (but with the 16 commissioners coordinating their work, and developing common positions, in a Conference of Data Protection Commissioners). The overall legal situation is therefore complex. However, there is full agreement, among the

[217] This section draws heavily on information kindly provided by the Data Protection Commissioner for Schleswig-Holstein, Dr Thilo Weichert, and his staff, including Messrs. Holger Brocks, Lukas Gunderman and Thorsten Koop.

Länder and between the *Länder* and the *Bund*, on basic principles: they flow from the German Constitution.

This brings us to the second point, which is that there is, in Germany, a strong tradition of data protection. This goes back to the Constitutional Court's 1983 Census judgment.[218] As the name says, the judgment concerned the collecting and use of personal data for a census; in it, the Court set out the basic constitutional requirements of data protection, and these have thus been entrenched in German law. They are discussed in section A.2.

However, the same trends that are notable in the United Kingdom can also be discerned in Germany: the federal authorities increasingly seek to get a grip on matters formally within the powers of the state authorities; they also increasingly talk of coordinating government action (at different levels and across states), in particular in the context of "e-government"; and European initiatives are often cited as a reason for such interventions.

But in Germany, unlike in the UK, there is a strong political force trying to prevent such centralisation and linking of actions (and data): the local, regional and state authorities oppose excessive centralisation because it impinges on their historical and constitutional functions. This is in addition to the data protection authorities opposing unjustified data collection, use and exchange. Moreover, although data protection is not as "hot" an issue as it was in the 70s and 80s, there is still strong popular support for the underlying principles. Where commissioners and local politicians combine, they offer a strong safeguard against excessive, federal data sharing arrangements.

Example No. 1:

> Until 2004, welfare support (*Sozialhilfe*) was local, and individual welfare officers had considerable discretion. This led to variations in what was being granted: some people in some states or cities would be given money for (say) a fridge, where others were not given such pay-outs. The federal authorities felt they had to monitor this, to ensure more equal provision of services. They therefore designed forms, through which the welfare officers have to report on their actions, by sending data to Nuremberg which had previously only been held in Kiel. This in itself brought considerable change, since until then most had worked simply with paper files. Initially, the data were only demanded in anonymised form. But recently there was a sudden demand that they be in identifiable form, purportedly to allow for longitudinal study: the central authorities claimed that the data would still otherwise be handled anonymously. But this was strongly opposed by the Data Protection Commissioners, who insisted that the data should not be passed on in identifiable form. The demand for identifiable data has accordingly, for now, been shelved.
>
> A similar development has taken place for drugs advisers: they used to be local professionals, and formally still are, but through a reporting requirement are now

[218] Volkszählungsurteil, BVerfGE Bd. 65, S. 1ff.

forced to conform to standardised rules set at the federal level (although again they only send reports in anonymised form).

The Data Protection Commissioners oppose such developments because they undermine data protection principles as well as good practice, which requires professionals to exercise professional judgement and discretion. They stress that these two things go together: good data protection should reinforce good practice (see Section A.3 for further details).

A.2 Constitutional Principles

General Constitutional Principles

In its Census judgment, the German Constitutional Court derived a fundamental "right to informational self-determination" (*das Recht auf informationelle Selbstbestimmung*) from the more general "right to [respect for one's] personality" (*das allgemeine Persönlichkeitsrecht*), enshrined in § 2(1) of the Constitution. As further developed in subsequent cases, this means that individuals should know (or at least should be able to find out) who collects data on them, when and for what purposes; and that strict limits are placed on the collecting, storing, use and disclosure of personal data.

Particular emphasis is given to the principle of purpose specification and limitation (*Zweckbindung*): personal data may only be collected, stored and further used for "specified purposes". The German courts place a particularly strong emphasis on the need to define the purpose in question narrowly: thus, in the police sector, the collecting, storing and use of personal data cannot be simply justified by reference to undefined "police purposes", but must relate to a specific police task, such as countering a (real and immediate) risk to the general public, or investigating a particular crime, etc. Similar distinctions are made in respect of the work of social services and educational establishments: data collected for one of the various tasks of such agencies must, in principle, only be used for the specific task and not also for other tasks, even if carried out by the same body.

Any data collected and used by others than the individual concerned should furthermore be strictly limited to such data as are clearly necessary to achieve the purpose in question – there should never be any data collecting (or data disclosure!) 'just in case' the data may come in useful for some as yet unspecified purpose at some later stage. This also means that only the minimum amount of data necessary for the purpose may be collected and held (principle of data minimisation). In addition, personal data must, in principle and whenever possible, be obtained from the data subject him/herself, rather than from other sources.

Furthermore, since collecting, storing, using and/or disclosing data all constitute interferences with a constitutionally protected right (the right to respect for one's personality), there must be a statutory basis for such actions (principle of *Gesetzesvorbehalt*). The detailed regulation of data processing in any particular context

may be set out in subsidiary rules (provided these meet the constitutional requirements of course), but the basic authorisation for the processing of personal data in a particular context/by a particular agency for the performance of its particular tasks must be set out in primary (state or federal) legislation.

All these principles are constitutional principles: the general laws and special data protection provisions in special laws discussed in this paper give effect to them.[219]

Constitutional Data Protection Principles for Children

There are few, if any, Constitutional Court judgments on data protection for children. However, a recent ruling (to be precise, an inadmissibility decision) laid down some important markers.[220] The case concerned newspaper reports about the children of Princess Caroline of Monaco. The Court stressed that children need special protection, also in relation to the right to respect for their personality. Children do not just have a right to respect for their existing personality – they also have a right to *develop* their personality without undue interference. They have a right to "become a person**"**. Interferences with the still-developing personality of a child therefore require greater justification than interferences with the already-developed personality of an adult.

As just mentioned, the case was about interferences with this right through press reporting. However, in Germany, collecting, storing and using personal data on a person is a completely parallel kind of interference with the same right. It follows that collecting, storing and using (and disclosing) data on minors also deserves greater justification, and that the general data protection principles mentioned earlier should therefore be even stricter applied to processing of data on them.

Constitutional Data Protection Principles Relating to Consent

As noted above, the Constitutional Court bases data protection on the right to "informational self-determination". A person's own choices in respect of the use of his or her data are therefore very important: consent to data processing will, in principle, allow for the processing of any personal data to which the consent applies. However, at the same time, the purpose of data protection is to protect a person against interferences with his right to respect for his personality. The German courts will therefore not simply accept that any purported consent to processing will suffice. On the contrary: valid consent can only be given for (again, narrowly) defined purposes, for very specific actions, and only provided the person concerned was in a position to properly judge the implications of giving his or her consent, and was free to give his or her consent and not in any way forced or misled. Full informing of the individual is therefore crucial. The

[219] Many of these principles are of course now also part of European law, as set out in particular in the EC Framework Directive on data protection, Directive 95/46/EC, which in the UK is implemented through the 1998 Data Protection Act – which is why German law and practice is relevant to UK law.

[220] BVerfG, 1 BvR 1353/99 of 31.3.2000. The case was not admitted for full consideration because the Court felt that the basic principles had already been established in earlier constitutional case-law, and had been properly applied by the lower courts in the case at hand. The decision is nevertheless of importance for its succinct summary (and confirmation) of those principles.

Federal Data Protection Law furthermore stipulates that, in principle, consent must be given in writing; that, if consent for processing is sought together with "other declarations" (e.g. in a contract relating to a different matter), the consent for the processing is to be given special emphasis; and that, if sensitive data such as information on race, sex life or criminal matters is sought, the consent has to specifically authorise this (§ 4a(1) and (3) BDSG 2003).

The question of free consent is particularly important and raises difficult issues in contexts when consent for processing is made a condition for the provision of a particular service, especially if there is a position of dependency (as in employer – employee or school – student relationships) or other inequality (as in the relationship between a landlord and a prospective tenant). The basic approach is that if the matter for which consent is sought is closely related to the service in question, the dominant partner may seek it as a condition for the provision of the service. A simple example is the offer of a contract of employment, or of a tenancy, subject to consent for the obtaining of references. But if the consent is not directly related to the primary purpose of the processing, the giving of such consent may *not* be made a condition: consent obtained under such a requirement would be invalid. Thus, for instance, a bank may not make it a condition for the opening of a bank account that the customer agrees to have his account data analysed for the purpose of offering him or her special offers on insurance.

In assessing whether a person was in a position in which s/he could give free and informed consent, all the circumstances therefore have to be taken into account: the relationship between the data subject and the body seeking the data; the nature of the data; the uses (and disclosures) for which consent is sought and their proximity to the relationship between the data subject and the body seeking the data; the importance and possible effects of the processing for which consent is sought for the data subject; and of course, last but far from least, the capacity of the data subject to appreciate the import of his or her consent (taking into account the complexity or otherwise of the matter at hand).

These principles – which are applied equally at state and federal level – have special implications in respect of children and minors. The German commissioners will generally assume that a minor aged 16 is capable of giving consent for the receipt of marketing messages from a particular firm, but will generally not accept that a child of 12 can do so; as a rule of thumb, the age of 14 is often seen as an important threshold. From 18 a person is considered an adult and in principle fully competent to decide, also on data protection matters. However, the more important the consent is, the more demanding the commissioners will be in respect of the above kind of considerations. The Constitutional Court ruling in the case of the children of Princess Caroline of Monaco also clearly supports a strict application of these principles. A blanket all-purpose "consent" by a child or minor for disclosure of highly sensitive information in circumstances which may seriously affect their welfare, as sought for example in the UK Connexions form, would undoubtedly be regarded as invalid in Germany.

Constitutional Principles Relating to the Disclosure of Data

In the public sector in Germany, data may only be disclosed by one public body to another either: (i) with the express, valid consent of the data subject (as discussed above), or (ii) if a law either expressly requires or allows such a disclosure[221]. This appears to be similar to the position in the UK, but is more firmly applied. As we have seen, German law on "consent" relating to data processing is applied very strictly, taking account of the matter for which consent is given, the nature of the data, the use(s) to which the data will be put, and the specific characteristics of the individual whose consent is sought and his or her relationship to the person or body seeking the consent.

As concerns disclosures based on law, it follows from the data minimisation principle mentioned earlier that only such data may ever be disclosed as are "necessary" for the fulfilment of the task of the receiving body: the mere fact that data may be disclosed in principle under a law does not "open the floodgates" (so to speak); rather, the necessity of the disclosure of specific data to the specific recipient for a specific purpose must still be established. This is further illustrated in Section A.3.

Furthermore, if data are obtained in the context of a relationship of trust, the resulting duty of confidentiality must be balanced against the possible duty (or permissibility) of the disclosure, and will generally count against such a disclosure unless there are clearly overriding reasons to disclose the data. As we shall in Section A.3, below, the data protection authorities emphasise that such trust is often an important factor in the capability of a professional or organisation (such as a doctor, or social services) to function well. Breaking such trust therefore requires particularly serious reasons. In view of the ruling by the Constitutional Court in the case of the Monaco royals, this applies *a fortiori* if the "entrusted" data (*anvertraute Daten*) relate to minors.

The crucial general point to be made here is that these (constitutional) tests in principle require an individual, case-by-case assessment.

Limited exceptions exist with regard to the establishment of "joint processing operations" (*gemeinsame Verfahren*) and "on-line processing operations" (*Abrufverfahren*), as well as for centralised "shared [federal/state] databases" (*Verbunddateien*). Joint processing and on-line operations are subject to special regulation in the national data protection law of Schleswig-Holstein and, in these, are treated with extreme caution, as will again be discussed in section 3, below. Shared federal/state databases are extremely rare and in practice, until now, limited to federal/state police purposes only. The best-known one is

[221] The discussion here is limited to disclosures between public-sector bodies, because the bodies involved in the kind of activities addressed in this study are still mainly state bodies. This also applies to schools (note that the main Protestant and Roman Catholic churches, which run many schools, are regarded as public-sector bodies in Germany). In any case, if a private body carries out public functions, it must, in Germany, in any case be treated, for data protection purposes, as a public body. The principles summarised here are reflected in both the Federal Data Protection Law of 2003 (*Bundesdatenschutzgesetz* 2003 or BDSG 2003) and in the various State Data Protection Laws (*Landesdatenschutzgesetze*). On the way in which they are applied in practice in the State of Schleswig-Holstein, see section 8A.3, below.

the so-called "INPOL" database maintained by the Federal Police Bureau (the BKA); it has been criticised for being unconstitutional.[222]

An attempt was recently made to establish a joined (federal/state) database for driving licences. Until now, driving licences are issued locally (at state level). The data are entered into a local database, but can be read (only) by the sister-licensing authorities in the other states. The federal government proposed that there should be one central database, into which all the 15 state licensing authorities would enter data, but which could be amended (and even deleted) by all. The Commissioners strongly criticised this plan, on the basis that there would be no clarity about who was in charge of what data, and thus no serious supervision or control. The plan has, for now, been shelved.[223]

A.3 Applying the Constitutional Principles in Practice: the Example of Schleswig-Holstein

The General Statutory Framework at State Level

In Schleswig-Holstein, as in other German states, the various agencies working with children – schools/education services, child welfare/social workers (*Kinder- und Jugendhilfe*), health, police, etc. – still work in principle separately on each child. This is considered right, because they each have different aims: schools want to educate a child as well as possible; social workers want to provide the best possible social conditions for the child (and its family); the police want to clear up crime. Each agency will of course need data on each child within its care or which is subject to its attention, in order to perform its respective task. Each agency therefore needs a special statutory basis for its personal data collection and use – as for any disclosure of their data.

In addition (and unless those special rules provide otherwise), they must of course comply with the general state data protection law (the *Landesdatenschutzgesetz* of the State of Schleswig-Holstein, or LDSG-SH for short). This general law will not be discussed in any detail here: suffice it to note that its general principles reflect the federal constitutional principles mentioned earlier (in some ways the law is more precise and stricter). However, its provisions on disclosures of data from one public body to another, and on data sharing arrangements should be noted. The first are set out in § 14(1) LDSG-SH. This allows data disclosures in principle: (i) when the data subject has given his or her consent; (ii) when the LDSG or another law expressly allows it; (iii) when the data are "necessary" for the fulfilment of a statutory task of the disclosing or the recipient body; or (iv) to protect "vital interests" of the data subject (e.g., when the data subject is

[222] One of the reasons for this alleged unconstitutionality is that it has been clear for a very long time (several decades!) that under constitutional principles there should be a special police data protection law (see above). But because of the sensitive political implications, no such law has been adopted. For details, see D Korff, A "seamless" system of data protection in the EU, Study for the EU Commission, 1995, and in particular the report on police and data protection in Germany, prepared in the context of that study.

[223] cf. also the recent suggestions that school student data be passed on to the central (federal) authorities, mentioned in section A.3, below.

in coma in hospital). However, this general provision is subject to the more specific rules in special laws which, as we shall see below, in fact impose much stricter conditions.

The rules on data sharing arrangements are set out in § 8 LDSG-SH. They apply to:

- automated processing operations which allow several bodies to jointly process personal data (*gemeinsame Verfahren* or "joint processing operations"); and to
- automated processing operations which allow several bodies to disclose data on-line (*Abrufverfahren* or "on-line processing operations").

The provision stipulates first of all, in general terms, that such operations "may only be established insofar as their establishment is proportionate,[224] taking into account the legitimate ['protection-worthy'] interests of the persons concerned and the tasks of the official bodies concerned." The importance of this stipulation becomes clear from the attached procedural requirements: the law stipulates in § 9(1) that the establishment of such joint or online operations is subject to a "prior check" (*Vorabkontrolle*).[225] This prior check can, in principle, be carried out by an in-house data protection official, appointed by a public body to ensure compliance for its operations with the relevant data protection laws and –regulations (§ 9(1)).[226] However, in Schleswig-Holstein, a relatively small *Land* with relatively small public bodies, this is unusual. In that case, the Independent Data Protection Centre must carry out this prior check. This means that the Schleswig-Holstein Data Protection Commissioner can effectively prohibit the establishment of a joint or on-line arrangement if he feels that it poses an unacceptable (disproportionate) risk to the rights and interests of the data subjects. It will be clear from the later sections in this paper that the Commissioner will be very reluctant to allow automatic sharing of any data on children; at most he might allow (say) basic name and address data to be exchanged in this way. He has to date not even been asked to approve such an arrangement: co-operation between different bodies working with children are all based on much more limited arrangements for (at most) limited data disclosures in individual cases (see Section A.3 for the most important examples).

In any case, data sharing arrangements of the above-mentioned kind will have to comply with a number of important requirements. For joint operations, the "processing particulars" (*Verfahrensverzeichnis*) that have to be drawn up (and usually notified to the Commissioner) must include also "the areas of processing for which each of the parties to the arrangement is responsible" (§ 8(2) LDSG-SH). This means that it must be clear

[224] *Angemessen* – the term also translates as "appropriate".
[225] Note that a "prior check" is required under the EC Framework directive on data protection for all processing operations "likely to present specific risks to the rights and freedoms of data subjects" (Art. 20(1) of the Directive). The UK DPA 1998 allows the Secretary of State to impose such checks for operations specified in an order – but no such order has as yet been issued and no operations in the UK are therefore subject to this requirement. In other words, the Schleswig-Holstein legislator feels that all joint or online operations are, *ipso facto* "risky", while the UK legislator has no such qualms.
[226] The institution of the in-house data protection official is an established German institution, used especially in the private sector, but has been formally recognised also in the EC Framework directive (see Art. 18(2), second indent, of the Directive). In Schleswig-Holstein, the in-house data protection official for public-sector bodies is regulated in § 10 LDSG-SH.

which body is responsible for which part of the processing operation. However, data subjects can contact any of the bodies involved in the exercise of their rights (such as the right of access, correction or erasure); if they make the request to a body that is not responsible for the area (and thus for the data) in question, that body must pass the request on to the body that is responsible.

If joint processing operations lead to the disclosure of data (from one of the parties involved to another, or from one of them to a body that is not party to the joint arrangement), the recipient, the time of disclosure, and the data that are disclosed must be recorded; the record of such disclosures must be kept for one year (§ 8(3) LDSG-SH).

With regard to on-line operations (i.e. on-line accessible databases), any body that accesses (and downloads) any data is responsible for ensuring that this action complies with data protection rules (in particular, that the data are necessary for the performance of the task of the body in question). The body that uploaded the data is not responsible – except that it should carry out checks on the permissibility of the downloading if it finds reasons to do so (*Anlasskontrolle*). However, it is required to carry out spot-checks to see if there is such cause (§ 8(4) LDSG-SH).

But as noted earlier, in practice no such joint or on-line systems have been established, or are likely to be allowed to be established, in the areas of interest to this study. Data disclosures and exchanges in these areas must therefore be assessed under the general rules on disclosures in the *Landesdatenschutzgesetz* and (more importantly) under the special data protection rules in the special laws covering the specific activities concerned.

For schools, these rules are set out in a provision on "data protection in education" (*Datenschutz im Schulwesen*) in the Schleswig-Holstein School Law (*Schulgesetz* or SchulG-SH for short). The provision in question, § 50 SchulG-SH, is detailed: it contains 10 sub-clauses and runs to just over 3 pages. Even so, the provision has been further elaborated on in a School Data Protection Regulation (*Datenschutzverordnung Schule*),[227] which includes an annexe listing the data that schools may collect and process in yet further detail. The list is quite limited. For instance, the only data that may be held by schools on the parents of children at the school are name, address and telephone number (or similar: this presumably allows the email addresses of the parents) (§ 50(1), at 2, SchulG; repeated in nos. 2.1–2.3 in the annex to the regulation). The results of "school, medical, school-psychological, or school-pedagogic examinations" (i.e. examinations by the doctor, psychologist or educational experts attached to the educational service) may be kept on file but may "under no circumstances" be entered on a computer database (no. 3.20 in the list). With one exception, the data appear to be purely factual (what exams are taken, marks, absence from school, etc., etc.). The exception is "learning behaviour and behaviour in the school" (the last number, no. 6).

Social work is regulated in the federal Law on Social Work (*Sozialgesetzbuch* or SGB for short). The general rules and purposes of this work are contained in Book I (*Buch I*) of

[227] The full name is *Landesverordnung über die Verarbeitung personenbezogener Daten in Schulen of 3 April 1998*, as amended on 22 February 2002.

this statute, the rules relating to work on children in Book VIII (*Buch VIII*, also referred to as SGB-8). The latter sets out in great detail the various tasks and purposes of social work for children: supporting families, supporting educational development, help in parental access arrangements, etc., etc. Chapter 4 of Book VIII (comprising §§ 61 – 68) deals with "protection of social work data" (*Schutz von Sozialdaten*): it sets out when what data may be collected; what data may be recorded; when data may be disclosed to others and how they may be used, etc.[228] These rules are strict. The law thus stipulates, for instance, that "data that are collected for different tasks of [a particular] state youth social work office may only be combined if, and to the extent and for as long as, this is necessary in relation to a direct connection [between those tasks, in the particular case]." (SGB-8 §63(2)).

The work of the police in relation to the investigation and prosecution of criminal offences is regulated in the Criminal Procedure Code (*Strafprozessordnung* or StPO for short). This contains a general provision, § 161(1)(new), which allows the police (acting under the supervision of the procuracy [*Staatsanwaltschaft*] "to demand information from all public bodies ... unless other laws or regulations regulate their competences more specifically." The qualification expresses the general legal principle *lex specialis derogat lex generalis*, or: a special legal rule overrides a more general rule. The crucial point is that the special rules in the School Law and in the Law on Social Work, mentioned above, are regarded as exactly the kinds of *leges generalis* in relation to the Criminal Procedure Code as are referred to in § 161(1), as further discussed below, at 3.2. They therefore override that paragraph: data can thus only be disclosed to the police by schools and social workers to the extent that the special rules on data protection in the special laws relating to their work allow this.[229]

It is also worth mentioning here a matter that is not strictly speaking to do with data sharing, but with the collecting of data by the police on children below the age of criminal responsibility (in Germany, that is 14 years). It concerns proposals from the government of the state of Hessen to allow the taking of DNA samples by the police from children under 14 years old who are known to the police as "child-thieves" (*Klaukinder*). The approach of the German (or at least the Schleswig-Holsteiner) data protection authorities to such proposed measures – and more generally to the storing of data on minors – is clear from the following comment by the Schleswig-Holsteiner Data Protection Commissioner, Dr Weichert:

Example No. 2:

> "The plans of the State Government of Hessen to store genetic fingerprints of so-called 'child-thieves' below the age of criminal responsibility has nothing to do

[228] It should be noted that the law stipulates, in § 61(3), that if private child welfare organisations are involved in the work covered by the law, measures must be taken to ensure that they, too, comply with the data protection rules in Chapter 4 of Book VIII in this regard.

[229] See further below. Note that this is again basically the opposite from the situation in the UK where, under the UK DPA, authorities of this kind can (and indeed often must) disclose data to the police whenever a statutory (or subsidiary) rule "requires or allows" it.

with protecting the public from harm or with prosecuting crime [the two main police tasks – DK] and especially nothing with the proper pedagogic handling of children-at-risk. It is the expression of a dangerous law-and-order populism and of the false belief that data hoarding [*Datensammelei*] will create more security. 'Child-thieves' cannot be brought to justice through the taking of tissue-samples, let alone be scared off. The establishment of a DNA database on children below the age of criminal responsibility would mainly have the effect of early criminal stigmatisation of children who need social-pedagogic help rather than a criminal tag for the rest of their lives." (Thilo Weichert)

(Datenschutz Nachrichten 1/2004, p. 22)

Inter-agency Co-operation and the Disclosure and/or Sharing of Data

Although (as noted above) considerable store is set by the independence of the different agencies, because they work for different purposes, it is of course also recognised that, precisely in order to fulfil their tasks properly, the agencies must, from time to time, have to work together – and that there are therefore circumstances in which data can be disclosed from one agency to another, or perhaps even shared more broadly. However, in line with the rules just mentioned, this is subject to two main considerations.

First of all, data disclosures between any of the agencies mentioned above (or indeed any public bodies in Germany) must always comply with all the relevant rules, as briefly mentioned there. Thus, if one agency wants to pass on data to another agency (say, a school wants to involve a child social worker), the first agency (the school) must, under the rules applying to it, be allowed to pass the data on, and the other agency (youth care) must be allowed to collect and store the data under the rules relating to that other agency. Secondly, it is a fundamental principle that such data disclosures or sharing can only ever be permissible in individual cases, on the basis of a case-by-case assessment of the need for such arrangements.

Even then, the basic data protection principles should be taken into account in establishing the modalities of such arrangements. Thus, even if it may be useful for a teacher to discuss a specific case with a social worker, and to disclose personal information in that context, it does not follow that the social worker (or his or her office) has a right to record the data on the child in question: that depends on whether the discussions disclose a need for the youth care team to become involved. Indeed, the teacher should consider whether it is necessary, in such an initial discussion, to reveal the identity of the child at all: it should be possible to discuss the case on the basis of anonymous data (or at least pseudonymous data, with the teacher knowing the identity of the child, but not the social worker).

These principles are reflected in the laws and regulations mentioned above. More importantly, given that these instruments by their nature remain rather complex, technical and abstract, the Schleswig-Holstein Data Protection Commissioner have given more specific, practice-related guidance on how the rules are to be applied in practice. In Section A.3, we shall briefly present three sets of guidelines issued by the commissioner

(or, in the last case, by the relevant ministry on the basis of advice from the data protection commissioner). Although these guidelines only relate to Schleswig-Holstein, and do not cover all possible forms of co-operation between all the agencies, between them they give a clear insight into how the data protection issues relating to such matters are (or at least should be) addressed in Germany generally. Before looking at these guidelines, it is useful to say a few words about the records kept by schools themselves and what happens when children leave one school and go on to another (typically, higher) school.

School Records

In Germany, there are three levels of schools for under-age children and young people: kindergarten (ages 3–6), lower school (6–12), and several types of higher school (12–18). The basic principle is (still) that each school has its own file for each student. There are (as yet) no central files, even at regional or state level (although there are mechanisms for ensuring that the state knows that children subject to the duty to attend school do in fact attend, and that the schools know what children in their catchment area are due to attend).[230] However, in line with the trend noted above, the federal authorities are now claiming that they need detailed data for a European co-operation system, PISA, and issued a form to be used for the passing on of the data. However, although for PISA only statistical data are required, the federal education ministry included a unique student number in the form. The Data Protection Commissioners pointed out that this was unlawful: in accordance with the constitutional principles set out earlier, such collection of identifiable data (personal data) requires a statutory basis. The federal authorities have since produced a draft of a regulation to this effect, but this set out the purpose of the data-gathering exercise in excessively vague terms and did not clarify why, for this purpose, identifiable data were needed. The Commissioners therefore concluded that the regulation would contravene data protection law and principles. The issue is therefore being reconsidered. For now, the situation remains that only schools keep personalised student records.

As noted earlier, the law specifies what data may be kept in those files. If a school wants to collect further data, it must ask for written permission to do so. Thus, a standard form prepared for schools by the Independent Data Protection Centre[231] lists first the basic data on students and parents which must be provided (with reference to the relevant legal provisions that require this), and then asks for their agreement to allow photographs of the child to appear on the school webpage (photos of identifiable persons are also personal data), and then, separately, for permission to include the student and parent contact details in a "chain-list", used to pass information on such matters as the safe arrival of children on a school trip (with one parent calling the next parent, etc.). The latter two matters are clearly optional.

[230] See § 50(4) and (5) SchulG-SH.
[231] The form is not binding: it is just an example of what a good form should look like, but in practice many schools have adopted it.

Crucially, the student files of different schools are kept separate: they don't follow a child through his or her school career. If a child goes from the lower school to a higher school (or from one lower or higher school to another one, e.g. because of a house move), the data are re-collected by the new school, and a new file is opened there. The files are destroyed no later than five years after the student left the school; it is usually done earlier. After that, the only record that is kept is that the child attended the school (with the dates) and the marks that the child obtained. If, in a rare instance, a school specifically wants to pass on data to the next school, it must either obtain the consent of the child and/or its parents, or follow the rules on inter-agency co-operation, discussed in the next section. Indeed, as far as moves from kindergarten to lower school is concerned, there should be no passing on of information without consent at all. As the Schleswig-Holstein Data Protection Commissioner writes in the guide on co-operation between schools and youth care agencies, discussed in the next section:

> *"It is not part of the tasks of kindergartens to inform schools about whether a child is fit to go to school. The aim of kindergartens is to facilitate the transition, to ease the child into school. Disclosure of data [from the kindergarten to the lower school] can lead to prejudice against the newly-enrolled child. It can therefore only be allowed with the consent of the guardians of the child."* [232]

Co-operation Between Schools and Youth Care Agencies

In response to debates in the Schleswig-Holstein Parliament, the Independent Data Protection Centre (which is the seat of the Schleswig-Holstein Data Protection Commissioner)[233] prepared a paper outlining the data protection requirements relating to co-operation between schools and the official (state) youth care agencies (*Jugendämter*).[234]

The Commissioner accepts that there will be occasions when a teacher notices that a student has problems outside school. In that case, the teacher should first discuss the matter with the student. However, if there are objective grounds to believe that this will not suffice to help the child, it may be necessary to inform the youth care agency, so that the latter can fulfil its statutory duty to provide help to ensure the proper bringing up (*Erziehung*) of the child, as provided for in §27ff. of the Social Work Law. However, the Commissioner stresses that (as mentioned earlier) consideration should first be given to a discussion with a youth case worker without identifying the child in question. He

---

[232] Paper on co-operation between schools and youth care agencies (op. cit.), p.5, somewhat freely translated.

[233] In Schleswig-Holstein the Data Protection Commissioner is fully independent, and thus fulfils the requirements of the supervisory authority provided for in the EC Framework directive on data protection. For historical reasons, the commissioners responsible for supervision of the public sector in some other states are not yet fully independent; some are part of state ministries.

[234] *Zusammenarbeit von Schule und Jugendhilfe – hier insbes. zu den datenschutzrechtlichen Anforderungen an die personenbezogene Zusammenarbeit, 2000* (the paper as published in the Commissioner's website is not dated, but it was written in response to a debate in parliament in 2000). In the paraphrase of this document in the text, detailed references to the law (in particular, to the LDSG-SH and the SGB) have been omitted.

points out that data protection law imposes no restrictions on such consultations; discussion of anonymous cases is therefore an easy, ready-to-hand option. Conferences can be held of teams of professionals from different agencies to discuss cases like this, anonymously, without any restrictions.

If more intensive exchanges relating to a named child or young person are thought necessary, consideration should first be given to obtaining the consent of the student. As the Commissioner points out, this is a professional imperative as much as a data protection one:

> *"Only by involving the person concerned can the trust be created or maintained, in relation to the school, to the youth care team or to other involved parties, which is required to provide effective help [to that person]."* [235]

All kinds of co-operative arrangements can be established with the active consent of the student. However, such consent can only be valid if the purpose of the co-operation and the associated data exchanges, the nature of the data and the extent of those exchanges, as well as the identify of the other agencies are all sufficiently precisely described to the student. The law requires that the student is also informed of the relevant legal requirements, of the fact that s/he is free to give his or her consent or not, and of the consequences of not agreeing. The consent must in principle be given in writing and must therefore be recorded (with the date, and details of the information provided). The consent can be withdrawn at any time: while this does not have retro-active effect, it would lead to the end of the processing (and thus to the end of the joined assistance). This too should be made clear to the student.

Young people can give such consent themselves, provided that they can assess the importance of the matter. Crucially:

> *"The assessment of the competence [of the child or young person] to assess this matter can only ever be made on a case-by-case basis, taking into account all the circumstances (age of the young person, psychological maturity, scope of the data processing, as well as scope, aim, recipient, time-period, sensitivity of the procedures). If a person under 18 years old can be deemed capable of making the decision, this overrides contrary wishes of parents or carers. However, if the latter have expressed such contrary views, a particularly careful assessment must be made, since this implies that the [proposed] co-operation between the school and the youth care agency has an effect on the relationship between the youth and his or her guardians. As far as children under the age of 14 are concerned, it has to be assumed, as a rule, that they do not yet have adequate capability to assess the often complex issues."* [236]

The Commissioner stresses that:

---

[235] p.2, at 2.
[236] Idem.

> *"co-operation between school and youth care agency in relation to a specific [young] person can only ever take place in a specific case. The necessity of the data exchanges [implicit in such co-operation] must be assessed with reference to each child or young person. General collecting of personal data from schools for tasks of the youth care agency, e.g. to determine the need for extra-curricular help, is not permitted."* [237]

Furthermore, in accordance with the constitutional principle mentioned earlier, the youth care agency should in principle always first seek to obtain whatever data it needs from the data subject (the child or young person) himself or herself (or, in the case of young children, his or her parents). It may only obtain data from another source – such as the child's school – in the cases envisaged by law, i.e. when the data cannot be obtained from the child or its parents because they refuse to give their consent even though the information is necessary to allow the youth care agency to fulfil its statutory task.[238]

The Commissioner distinguishes between the situation in which a youth care agency already dealing with a child asks the child's school for information, and the situation in which a school feels it should pass on information to a youth care agency of its own motion. He gives the following examples of situations in which a school may provide information to a youth care agency, at the request of that agency:

- the agency needs to know how a schoolchild behaves in class or *viz-à-viz* other children, in order to provide appropriate help to the child;
- a schoolchild is in an emergency or crisis situation and the agency needs the information to take the child in care;
- the parents decline an offer of help from the agency and thereby (in the view of the agency) endanger the child, in circumstances in which (under the Social Work Law) special care measures can be imposed (but if the agency is involved in a parental care decision in a divorce (or similar), it must seek the permission of the parents);
- if the agency has been asked by a court to provide a report on a child and the agency needs school information about the child in order to compile the report.[239]

A school can approach the youth care agency, and pass on information on a child to the agency, in the following cases (again given as examples):

- if the school has well-founded reasons to suspect that the child is abused, sexually abused or neglected;

---

[237] p.3.

[238] Data can also be collected from the school if the collection of the data from the child or its parents would involve a "disproportionate effort". However, under that test, only completely innocuous data such as contact details can be passed on; it does not allow for the passing on of information about the child's problems.

[239] p. 3, with reference to the specific statutory provision allowing the request in each of the cases mentioned.

- if the child commits serious acts of violence or other serious crimes in school (such as drug abuse), and the parents are demonstrably not capable of dealing with this behaviour [note that referral to the agency without the co-operation of the child and parents in such cases is thus limited to extreme cases];
- if the schoolchild is in an emergency or crisis situation in which the youth care agency can help, if the child at least agrees with the request for help from the agency;
- if the schoolchild repeatedly fails to attend school, or if there are serious learning, performance or behavioural issues, it can be appropriate to involve the youth care agency as a precaution, if the parents refuse to cooperate with the school.[240]

The law is more restrictive as concerns the passing on of data from a youth care agency to a school. This is because the data held on a child or young person by the agency may in principle only serve the purpose of care for the child or young person (i.e., may not be used to further the child's education generally). Specifically, because trust is essential for proper youth care, the "social data" in question are regarded as especially sensitive, and youth care workers are consequently subject to a particularly strict duty of confidentiality. In all but the most exceptional cases, the youth care agency should only pass on data on a child to the child's school with the consent of the child (or, in case of a young child, its parents). An exception (i.e. a case in which the disclosure of youth care data to a child's school without the child's or his or her parents' consent is absolutely essential, and should be allowed even though it may undermine the relationship of trust) can only exist when this is necessary to protect the child (or another person)[241] against a real and serious danger.

But these are exceptional cases: as the Commissioner points out, in principle the school (any school) should obtain its data on its pupils from those pupils, and not from others.

Similar duties rest on other bodies, including in particular private-sector bodies that may be involved with children. If a school passes data on to such institutions (even if this is with the consent of the data subject), the recipient bodies may only use the data for the specific purpose for which they were provided, and may not pass the data on any further. Furthermore, the school should limit the data it provides to its own tasks. A school may therefore, with the consent of a schoolchild or student, pass on information to a private "homework-assistance" body, but it should limit this to straightforward educational information (unless the student or his or her parents specifically requested further disclosures).

[240] pp.3–4. The Commissioner notes that under the School Law in Schleswig-Holstein there is never a duty on the part of a school to contact the youth care agency, even in such cases (this is different under the Bavarian law), but the cases listed are cases in which the school is allowed to involve the agency, at its discretion (always after due consideration of the individual case).

[241] The German text leaves the question open, but we assume that information can be passed on if, e.g. a child or young person being helped by the youth care agency makes serious threats against another person, of which the school should be informed.

Finally, the Commissioner points out that broad team meetings of different professionals involved with a child (also called *Hilfekonferenz* or "help meetings") are possible under § 36(2) SGB-8, in cases in which a long-term (multi-agency) assistance plan is drawn up with regard to the child. This is a "communicative process" involving the child, its parents, the responsible youth worker and "other professionals". But – precisely because in such team meetings a whole range of personal details can be disclosed – each of the professionals involved has to take special care in the handling of the data. Consideration should be given to having a small team with access to all the data, while consulting others without disclosing the identity of the child concerned (or at least without those others opening their own records on the case). The Commissioner adds that "*participation of a teacher in such a meeting is conceivable and useful*" (under these conditions).

Co-operation Between Youth Care Agencies and the Police in the Prevention and Fight Against Crime

In another paper, the Independent Data Protection Centre has set out the "outline data protection requirements for co-operation between youth care agencies and the police in the fight against and prevention of crime".[242] The paper takes the form of comments on guidelines in a co-operation agreement between the social services of Kiel and the police in the city. This co-operation agreement is a clear attempt at what in Britain is referred to as "joined-up government": the aim is to "join up" the social-work and police activities "at all levels" and to "co-ordinate" them in specific cases – albeit, of course, "within the limits of data protection requirements". The agreement envisages "regular co-ordination meetings" and even temporary postings (*Hospitationen*) of social workers and police officers in each other's offices. Contact persons are to be appointed to facilitate "quick and un-bureaucratic" contacts.

Integrated policies (*gemeinsame Handlungsstrategien*) are to be adopted, under which the police can report cases of "immediate risk" (*konkrete Gefährdung*) (such as cases of children and young people involved in crime, or subject to neglect or abuse, neglected homes, drug dens, etc.) directly to the social services. Conversely, the police is to receive information about individual children and young persons, and about individual families, from the social services, whenever this is "necessary for the provision of assistance by the social services" – but again, of course, provided that "this is compatible with data protection requirements". Indicators to this effect include, according to the agreement:

- violence in families, if it may be assumed that police intervention is necessary;
- a need for urgent measures in cases of children involved in serious crime;
- children in care homes who are likely to run away and should be quickly returned to prevent harm;

[242] *Datenschutzrechtliche Rahmenbedingungen bei der Zusammenarbeit von Jugendhilfe und Polizei bei der Kriminalitätsbekämpfung und –verhütung – Anmerkungen zu den Leitlinien für die Zusammenarbeit zwischen dem Amt für soziale Dienste (der Landeshauptstadt Kiel) und der Polizei (Polizeiinspektion Kiel) vom Oktober 1999, aktualisierte Fassung der Anmerkungen vom 11.07.2000, Az: 72.02/98.002*. Note that the requirements only related to the crime-prevention and investigation task of the police and not to the preventing-dangers task – what the British tend to call the public-order aspect of policing.

- when children or young persons are in danger and police intervention is necessary; and
- when families, children or young people agree to such co-operation.

Under the agreement, youth crime officers are to contact (the youth care office of) social services if a young person has been involved in five criminal acts in one year (but they may establish contact sooner in cases of serious crime). The police are also to inform the social services in some detail of decisions not to prosecute young people.

Finally, the agreement envisages the establishment of a joint social services/police "clearing and crisis intervention centre" for seriously delinquent children and young people. This is to involve the police, youth crime prosecutors, youth courts and youth probation services. The centre is to operate under the responsibility of the social services. The agreement stipulates that "data-protection rules and social-work confidentiality [*das Sozialgeheimnis*] will be fully respected in [this] co-operative endeavour."

The Independent Data Protection Centre welcomed "all efforts leading to an appropriate and legally acceptable reaction to youth crime *phenomena*" and the fact that the agreement recognised that compliance with the rules protecting social data (data held by the social services) was an essential pre-condition for effective youth care. But it then went to point out the strict limitations on the proposed data exchanges, and especially the strict rules on confidentiality to which the social services are subject.[243] Compliance with these restrictions very significantly restricts the seemingly broad co-operation and data sharing envisaged in the agreement (although it should be noted that even in its own terms, the agreement only ever envisages information disclosures in individual cases, after due consideration of the specific circumstances of the children or young people involved).

In accordance with the principles set out earlier, the test for any disclosure of information is whether the disclosure serves the statutory task of the disclosing entity, and is needed for the statutory task of the receiving entity.

Thus, one of the tasks of the police is to prevent danger (harm) to the public. The task of youth social work is "*to protect children and young people from harm to their well-being*" (*ihr Wohl*). Such a risk can arise from criminality against them, or from a danger that they themselves may become involved in criminality. The police can therefore, in appropriate cases, inform the youth social services of such risks. However:

> *"This risk must be sufficiently concrete in terms of its source, time and object. A vague suspicion that a risk might materialise is not enough."* [244]

The social services can then use the data to protect the child or young person in question from harm.

---

[243] In the paraphases below, detailed references to pages and legal provisions have again been largely omitted (but page references are given for passages quoted in full).
[244] p.3, under I.

Similarly, the police can, in order to prevent a risk of crime, contact a school (again, provided that there is sufficient, concrete cause to do so in a particular case). The school can then use this information to fulfil *its* statutory duty, which is "to prepare each schoolchild for its role as citizen endowed with relevant rights and obligations." And the police are specifically allowed to inform youth court support (*Jugendgerichtshilfe*) under separate guidelines aimed at support for first-offenders in particular, which allow for non-prosecution in cases in which, as an alternative, "additional education support" is offered where it is felt that this may prevent further criminal behaviour.

All of these matters relate to prevention of danger to the public. This must be distinguished from the separate police task of investigating criminal offences. The guidelines in the social work/police arrangements in Kiel are, on their face, only related to the former: they are not supposed to apply to police investigations. However, the Data Protection Centre's comments also address the latter matter (if only because, as it points out, issues of prevention may well arise in the context of a criminal investigation). It points out that until recently, and contrary to constitutional principles, there was no specific statutory framework for the processing of personal data in the context of criminal investigations.[245] However, § 161(1)(new) CPC (already mentioned earlier in this paper) now specifically authorises the prosecutor and the police acting under his authority in the investigation of crime "to demand information from all public bodies ... unless other laws or regulations regulate their competences more specifically." As already noted, the Law on Social Work provides particularly strong protection for "social data", and expressly stipulates that such data may only be passed on to any other body (or any outside person) where that law itself expressly allows this (§ 67d(1) SGB-10). This therefore also applies to the police.

The law allows the passing of basic data (name, date and place of birth, address and name and address of employer) to the police (§ 68(1) SGB-10). However, the police force is likely to already have these data, and in any case that is not the kind of information they are usually looking for in a criminal investigation; they would seek information about the personal situation of the young person. Such information cannot be passed on under that provision. Indeed, sometimes even address data cannot be provided under this provision, e.g. when the address is a care home, or women's refuge, or drug clinic.

Social services can pass on information to others (in theory, including the police) if the passing on of the data is "for the purpose for which the data were obtained" in the first place (§ 69(1), nr. 1, alt. 1 SGB-10). However, the purpose-limitation principle expressed in this provision must be strictly adhered to. The data will normally have been obtained to allow the social services to perform its functions, not to support the police. This provision therefore also does not normally allow for the disclosure of social data.

A further stipulation, in the same paragraph of the Law on Social Work, allows the passing on of data by the social services to "other bodies" when this is more generally

[245] The earlier general rules on police activity in the Criminal Procedure Code were not sufficiently specific in relation to data processing to meet the constitutional requirements.

necessary for the fulfilment of the task of the (social work) body that discloses the data (§ 69(1), nr. 1, alt. 2 SGB-10). This provision (the main one in the current context) in principle allows social services to disclose data (also) to the police, if that is necessary to fulfil the task of the social services (in the case of children, of the youth social services). For instance, it may be necessary to disclose some personal data to the police in order for the social services to ascertain certain facts about a young client. However, in any such cases, the social services must take the interests of the data subject (the child or young person) into account – as well as the more general interest of the social services themselves to work in conditions of strict confidentiality:

> *"In assessing when a disclosure [of information on a young client of the youth care agency] is necessary [for the task of the agency], a strict test is to be applied in view of the interest of protection the trust [between the youth and the agency]. Youth care comprises actions for the benefit of minors and their families. It seeks to promote the development of children and young people, to support or re-establish parental educational responsibility and to protect children and young people from threats to their well-being. Youth care is in particular based on the principle of voluntariness, i.e. the persons concerned can in principle determine for themselves what happens to their data. The success of (socia-)paedogogic work and advice depends inter alia on the existence of a safe area (ein geschutzter Raum), which can create the trust between those involved that is required for effective co-operation."* [246]

It may sometimes be necessary to pass on data on a child or young person to the police in order to prevent risks to the child or young person, e.g., when there is a risk of abuse by the parents, or if there is a serious risk that the child or young person slips into serious crime. However, even then the question will arise how useful the provision of information on the child is for the purpose of social work. The police may not have a choice other than to prosecute, irrespective of the social conditions (*Lebenssituation*) of the child – even if prosecution (of the child or of a parent) is not in the child's best interest from a social service point of view.[247] It is unclear how involving the police will therefore contribute to the aims of the social services. Under the Law on Social Work, information on a child may only be passed to the police in the context of criminal investigations if this helps to fulfil (or at least does not undermine) the task of the social services, i.e. if it is in the interest of the child to do so, even if this may lead to prosecution. This clearly requires a careful balancing of interests in each individual case.

In this balancing exercise, the wider interest of the social services in maintaining confidentiality should also be taken into account:

> *Passing on of data [on a child or young person] can deter the person concerned from seeking further help from the youth care agency. It is quite possible that the agency was contacted precisely in order to resolve or lessen the problems with an*

[246] p.5.
[247] In Germany, prosecution policy is based on the "principle of legality" (*Legalitätsprinzip*), under which all criminal offences that have been detected must, in principle, be prosecuted.

> *(offending) young person without involving the police. Often, and in particular in relevant parts of society, there is a fundamental reluctance to engage with the police. The assurance of confidentiality often plays a big part in the success of the help offered. Passing on information to the police will often undermine the chances of success.* [248]

This applies in particular in respect of information concerning personal and educational help. Such data can only be passed on when the individuals concerned give their consent, or when a court needs the data to protect a child, and in other extremely narrow circumstances. And even then the question has to be answered – by the youth care agency – whether this will actually be helpful to the child.

The law is also strict as concerns the situation in which a social worker learns of the commission, or planned commission, of criminal offences:

> *A child social worker who learns of the planned commission of a particular, serious crime, is required to pass this on to the police ... If however s/he learns about an already-committed crime, then s/he is not required to inform the police, because the duty relates only to protection [of the public] from danger (die Abwehr eines akuten Gefahrs) and to prevention of a specific crime, not to criminal investigation. In certain circumstances it may suffice to only warn the person in danger. In cases of (even serious) planned crimes there is furthermore no duty to inform the police if another measure, such as trying to dissuade the perpetrator from his actions, or warning the intended victim, is possible.*[249]

Social services are in principle required to provide information to the courts, if ordered to do so by the court in question, but even then this may be subject to some special qualifications in respect of particularly confidential data. The courts cannot order the social services to disclose data to the police. The general youth social services can also participate in the special youth care services attached to the youth courts (*Jugendgerichtshilfe*), but even then must always give priority to their overall aim of helping the child or young person in question. What data are passed on, even in these special circumstances, therefore still remains, to that extent, a matter for the social services to decide. This too cannot be used as a basis for disclosures of information to the police.

Mention is furthermore made of the (multidisciplinary) "team conference", already referred to in the previous section, in connection with co-operation between schools and social services. The Data Protection Centre stresses that such teams should in principle discuss cases anonymously. If this is impossible and they need to discuss individual cases by name, they should obtain the consent of the client (i.e. for youth care services, of the child or young person and, where appropriate, its parents). The Centre feels that participation of a police officer in such a team is "conceivable", but questions what kind

[248] p.5.
[249] p.6, references to legal provisions omitted.

of help the police can offer (given that the aim of the conference must remain help for the child or young person, rather than police action such as prosecution).

Finally, it is also not necessary – and therefore not allowed – to pass on identifiable information to the "crime prevention councils", which on the basis of past experience seek to develop new crime prevention initiatives. Scientific research does also not usually require identifiable information.

Co-operation between Youth Care Agencies and other Agencies in Relation to Domestic Violence, Sexual Abuse and Violence Against Children and Young People

Finally, mention should be made of a detailed brochure with "guidance and tips" on how to deal with data protection matters in relation to violence in the family, which is shortly to be issued by the State Ministry of [Social Affairs] of Schleswig-Holstein, and which was prepared by the Independent Data Protection Centre.[250]

The introduction to this brochure addresses the fundamental tension between the need for co-operation, the need for confidentiality and trust, and data protection. It is useful to set out these considerations in full: they give a good insight into the basic approach to this complex of issues by the German authorities:

> *The tasks of the youth care agency [Jugendhilfe] often overlap with those of other institutions and professions, such as the police, the prosecutor, family courts, schools, psychiatrists, doctors. The tasks of the youth care agency in particular touch on those of the other institutions in the areas of domestic violence, sexual abuse, physical abuse of children and young persons, and youth crime. In these areas there is an interest in the exchange of information in order to provide the best possible measures and to ensure effective co-operation between all the institutions and professions involved. At the same time – given that a relationship of trust is often a decisive factor in the provision of help – the institutions providing help have an interest in maintaining the confidentiality of their own data. Data protection law is one of the means to try and create the (right) balance between these conflicting interests. However, often, data protection is seen as an obstacle to effective co-operation and sometimes even as a barrier preventing professional action. These reservations vis-à-vis data protection are*

[250] *Datenschutz und familiäre Gewalt – Hinweise und Tipps zum Datenschutz bei Kooperationen zwischen dem Jugendamt und anderen Stellen, insbesondere im Bereich der häuslichen Gewalt, des sexuellen Missbrauchs und der Misshandlungen von Kindern und Jugendlichen*, due for publication later in 2006. An annexe to the brochure contains pretty much all the provisions of federal and state law quoted in this paper. In the text, we have only occasionally referred to specific provisions; full details are given in the brochure. The summary in this paper focuses on matters of relevance to the ICO study: some matters (such as the passing on of information from youth care agencies to the specialised court youth care agencies, are dealt with very briefly only, if at all, even if they are addressed in detail in the brochure. Conversely, on some matters – in particular, on the issue of consent by minors – we have somewhat elaborated on the information in the brochure, in consultation with the Independent Data Protection Centre.

caused by the extent and complexity of data protection rules, which are difficult to know and understand for both lawyers and non-lawyers, and which therefore often create confusion in the minds of all involved.

The catchphrase "data protection overrides child protection", which is often invoked in connection with problems of co-operation, is not correct. The guarantee that personal data are protected is a condition for professional action; in many cases such action would be impossible without it. In practice in the youth care field situations rarely arise in which a disclosure of personal data is not permitted although it is needed – because as a rule data can be disclosed either with the consent of the data subject or when the disclosure is necessary to prevent harm to important and legally protected interests. If it can be difficult in specific cases to obtain the consent of the data subject or to assess the risk of harm, then that is not a data protection problem but a difficulty that manifests itself in youth care practice in many ways and that should be resolved at the professional level.

It has to be admitted that the youth care agency is a state institution and has a "guardian" role in respect of its clients, and is thus subject to more restrictions on the obtaining of the consent of its clients than non-state agencies.[251] *On the other hand, the youth care agency has been granted special rights to pass on personal data without consent.*

The problems of co-operation between the different institutions do not arise from (what seem to be) data protection problems, but from the different tasks and [different] operational approaches of those involved. It is therefore a fundamental requirement of good [inter-agency] co-operation that all the partners are sufficiently aware of the tasks of each of the other partners, and of the way in which they fulfil these tasks. In addition, all such partners must be adequately knowledgeable in data protection matters, so that in the framework of co-operation between them there is clarity about what data they may or must pass on and what data they must keep confidential. If there is such clarity about the respective tasks of the partners and about the data protection requirements relating to their activities, this will result in a clear reduction of the potential for conflict in their co-operation arrangements. What is more: it is precisely through the eradication of misunderstandings that the conditions for successful co-operation by all involved are created.[252]

The brochure reiterates that the special rules applicable to the youth care agency – and in particular the special data protection rules, already discussed above – as *leges speciales* override any more general rules in the federal or state data protection laws; and that "social data" (all data – including opinions and evaluations in individual cases – relating to the clients of the social services that are "entrusted" to the social services, i.e. provided to them in the context of a relationship of trust) are subject to special protection and

[251] Under German law, state agencies cannot ask citizens for consent for the processing of data which they do not need for their statutory tasks – DK.
[252] pp.1–2.

confidentiality.[253] Even so, there are many rules that allow the disclosure of data (including, in special cases, of "entrusted data"), and it will furthermore often be possible to obtain the consent of the data subject. In practice, disclosures are therefore often possible – the point is that the matter should be carefully assessed, in the light of the relevant rules, in each case.

Furthermore, consideration should be given to disclosing data in anonymous or pseudonymous form: if the purpose (e.g. of obtaining the view of another agency on a case, without necessarily involving the other agency further) can be achieved in this way, the disclosure should be limited to such anonymised or pseudonymised disclosures. Another advantage is that "entrusted" data (which can only be disclosed in special circumstances, as just noted) can be quite freely disclosed to another agency in anonymous or pseudonymous form, if this serves the interests of the youth care agency.

Consent

The question arises as to who, in appropriate cases, should give consent for the disclosure of data held by the youth care agency. The brochure points out that this is not always the data subject: it can be another person who informed the agency in confidence, for example a neighbour reporting on suspected abuse next door. In that case, the agency should check with the informant what data the latter wants to be treated in confidence: if the neighbour only wants his or her identity to be kept confidential, the information about the abuse itself is not confidential and may, therefore, be passed on to the police (for instance), if the youth agency believes that that is in the best interests of the child or children concerned.

On consent more generally, the brochure repeats the clarification already contained in the guidelines discussed earlier: that valid consent can only be given by a person if the person was adequately informed of the purpose of the processing and of the nature and scope of the data to be disclosed as well as of the recipients of the data. "Consent for all cases is not valid, because the data subject cannot assess who will find out what when about him."[254] The data subject must also be informed that s/he can at all times withdraw his or her consent, with effect from that moment (but not retrospectively).

On the obtaining of consent from children and young people, the brochure (like the guidelines discussed earlier) stress that their capacity to give consent must be assessed in the light of (amongst other matters) their age, mental maturity, scope and importance of the processing (i.e. of the impact that the disclosure can have on them), the recipients, and the sensitivity of the data. The authors feel that "often, the required capacity will exist from the age of 14 years".

---

[253] The brochure clarifies when information is to be regarded as "entrusted" (subject to a special duty of confidentiality). This is not only the case if the person providing the information expressly stipulated it, but can also be clear from the circumstances. If a parent shows a youth care worker something (e.g. bruises on a child), the parent may expect confidentiality; similarly, if a parent tells a kindergarten teacher of abuse and the teacher reports this to the agency. But if the teacher informs the agency of bruises on a child which the teacher noted themselves, this is not "entrusted" information (unless the teacher specifies it). (pp.7-8).

[254] The "who ... when ... what" is a reference to the Census-judgment discussed at 8A.2, above.

But according to the Independent Data Protection Centre, if extensive, sensitive data are collected from a child or young person (e.g. on whether s/he is sexually active, or uses drugs, or is involved in other criminal activities), and/or if it is proposed to share this information widely with other agencies, with unknown repercussions, this will normally not be the case. If the child is not capable of giving informed, considered consent (e.g. in such cases), the parent or legal guardian must be approached. It would in any case be inappropriate to ask a child or young person to provide data not just on him/herself but also on other family members (parents, siblings) – especially if the information is intrusive, e.g. as to drug abuse by parents or siblings, or sexual matters, or the financial situation of the family, and more especially if it is intended to disseminate the data to other agencies. Such indirect data-gathering on the other family members would contravene the principle that personal data must be obtained directly from the data subject (unless the matter is trivial – which is not the case with the kind of information just mentioned).[255]

The brochure points out that obtaining of consent makes life considerably easier for the (youth) care worker or other professional in question. However, while they may point out any possible negative consequences of a refusal to give consent, they should never put such pressure on the person concerned as to rob the "consent" of its voluntary aspect: consent given under duress is not valid, and any processing of data on the basis of such consent is thus unlawful). Thus, they may point out to the neighbour reporting child abuse that unless s/he agrees to his/her identity being disclosed to the police, the latter may not be able to bring a prosecution. Similarly, if one parent reports that his or her partner abuses a child, the care worker may point out that if s/he does not co-operate by allowing the involvement of other agencies through the disclosure of the information s/he provided, this may mean that further-reaching protection measures may have to be taken than if s/he did agree to the disclosure. But such pressure should always be applied with great care. In cases of obtaining consent from children, even relatively minor pressure from a person in authority will invalidate any "consent" that the child may give.

Disclosure of "Non-entrusted" Data (Data not Subject to Special Confidentiality)

A youth care agency may use any "non-entrusted" data it obtains for the specific task for which they were obtained (e.g. to assist a young drug user to overcome his or her addiction) and for other tasks of the same agency, e.g. to help the client in educational matters (§ 69(1), no. 1, 1st alternative SGB-10). The agency may also pass on such the data, of its own motion,[256] to other social service agencies and other agencies fulfilling similar tasks, such as state schools and kindergartens (§ 69(1), no. 1, third alternative SGB-10). However, as noted earlier, even for such data this is always only permitted

[255] The situation is different for information that happens to be provided by-the-by. But if data are specifically requested from a child or young person about other persons (parents, siblings or friends, or others), this constitutes "[targeted] collecting of data" (*gezielte Datenerhobung*) contrary to this principle.
[256] The question of disclosing data on demand, in particular to the police and prosecuting authorities, is discussed separately later, under the heading "disclosing data on demand".

provided the disclosure does not undermine the primary purpose of the youth care (§ 64(2) SGB-8). As always, this can only be determined by means of a careful assessment in each individual case. As always, consideration should always be given to involving the person concerned and obtaining his/her consent (and/or, in appropriate cases, the consent of the parents or guardians).

The third alternative in § 69(1), no. 1 SGB-10 can, however, not be used for the passing on of (even "non-entrusted") information to private schools or kindergartens (because they are not "providers of social services" [*Sozialleistungsträger*] in the sense of § 35 SGB), or to doctors, psychiatrists, psychotherapists, or to state agencies which are not "providers of social services" such as the police, the prosecution service or the courts. For co-operation with those there are other, special (and more restrictive) rules.

Disclosure of "Entrusted" Data:

"Entrusted" data can be passed on (also without consent) in limited circumstances, when there is a manifest risk to the child or young person, e.g. to a family court, if the data could have an impact on a decision of the court for which these data are needed (such as a custody order); to a new carer (if the previous one was informed); or if there is an immediate emergency; or if the youth care agency would be required to report the matter to the police. The last two are of particular interest.

Even in an emergency, careful consideration must be given to the specific circumstances and to the consequences of a disclosure:

> *In some cases there is authority to disclose [personal] data on the basis of the existence of an emergency [Notstand] in the sense of §34 of the Criminal Code (Strafgesetzbuch or StGB). [This provision] first of all requires that there exists an immediate danger to a legally-protected interest (i.e., here: sexual self-determination, physical integrity) and that the disclosure of the social data are necessary to prevent the threat from materialising.*
>
> *The provision furthermore requires that the interest to be protected (i.e. the health of the child) substantially outweighs the interest that is set aside (data protection). The disclosure must also be an appropriate means to counter the danger and the youth care worker must have honestly believed he acted to prevent the danger.*
>
> *If these conditions are fulfilled, the duty of trust is set aside and the ["entrusted"] social data may be disclosed, provided that in addition the general data protection conditions are fulfilled. For instance, the success of a youth social care measure may not be endangered as a result of the disclosure. Such a danger will arise if a youth care measure, which in the particular circumstances of the case is necessary and required, can no longer be applied as a result of the disclosure. This is the case, for instance, if certain people who until then had co-operated [with the youth care agency] would subsequently refuse all co-operation and would thereby make appropriate help [for the child] impossible.*

> *It should not be automatically assumed that an emergency situation in the sense of §34 StGB exists whenever child abuse comes to the attention [of a youth care agency]. Rather, there should be a careful assessment in each individual case to see if, first, there is an immediate danger and, secondly, if the measure [i.e. the disclosure] is necessary to prevent the danger from materialising.* [257]

Both these conditions are further clarified, as are the criteria that flow from them.

Immediate Danger and Disclosures to the Police (of the Agency's Own Motion)

As far as the question of immediate danger is concerned, a social worker should not automatically assume from the fact that there has been domestic violence in one instance, that further abuse is likely or imminent. On the other hand, sexual abuse of children is typically serial – and in that case, a youth care worker can often assume further danger from established past abuse. As always, a careful assessment of each particular case is required.

The duty to report offences to the police (laid down in §138 StGB) is limited to *specific*, *serious future* crimes, such as murder, manslaughter, kidnapping, hostage-taking, and robbery with violence. Information on *minor* or *past* crimes therefore need not be – and thus in most cases may not be – reported. In the vast majority of cases handled by youth care workers – which will of course not involve such major crimes – §138 StGB can therefore not be relied upon as a basis for passing on information to the police.

§ 34 StGB – the provision on "immediate danger" – also does not provide a general basis for disclosures to the police: it is aimed at averting that danger, not at facilitating police investigations of prosecutions. But if bringing charges can help to avert an immediate danger to a child, it can be relied upon. Once again, that is a matter to be assessed on a case-by-case basis by the youth care worker in question. Mere suspicion does not suffice, however; in that case, the youth worker should first investigate the case further. Data collection to this end should of course conform to the data protection requirements.

Necessity of the Action

The second condition for the applicability of § 34 StGB is that the measure in question is "necessary" to avert the (immediate) danger. This means that two further conditions must be fulfilled: the measure (i.e. providing information to the prosecuting authorities) must be capable of averting the danger; and it must be the least harsh (mildest) measure available to avert the danger.

[257] pp.10–11. In German, the emergency discussed is referred to as a "justifying emergency" (*ein rechtfertigender Notstand*), i.e. an emergency justifying the setting aside of otherwise-protected rights. The additional conditions set out in the second paragraph of the quote are, in the original German text, contained in a footnote.

On the first point, the brochure points out that reporting sexual or other abuse to the police does not necessarily lead to actions that protect the victim (such as removing the suspect from the latter's proximity). For instance, there may be insufficient evidence to arrest the suspect. To that extent, informing the police may not even be suited to achieve the aim of protecting the child. Secondly, the effect of reporting to the abuse must be assessed: it may have negative repercussions, also for the victim. Other measures, not involving the police, should therefore also – indeed, first – be considered.

Resulting Criteria

It follows from the above that in all instances, youth care workers must carry out a careful balancing act. In this, there are arguments for and against informing the police. At the heart of this assessment should always be the consequences for the child and for the measures in support of the child.

Arguments for informing the police can be:

- that a criminal trial can assist the child in overcoming the past;
- that the perpetrator can be removed from the child by detention and imprisonment, or simply deterred from further abuse by the mere fact of being reported to the police;
- that if the matter is not reported the perpetrator will continue to have access to the child (and perhaps other children).

Arguments against informing the police can be:

- that other individuals will side with the perpetrator and that family ties may be irreparably damaged;
- that the child can be blamed for having "destroyed the family";
- that the child will feel that the (inevitable) questioning puts his or her veracity in doubt and may therefore lead to secondary victimisation;
- that by passing on the information to the police the relationship of trust between the youth care worker and the child is undermined.

The last issue – protection of trust – is a fundamental condition for effective help, but even so is not always conclusive. Serious danger from possible sexual or physical abuse cannot be a price paid for such trust. In the end, it would also damage the relationship between the child and the youth care worker if the former gained the impression that the latter tolerated continued abuse.

Data Protection Within the Youth Care Agency

The brochure points out that even within the youth care agency, personal data must not circulate freely but rather should be limited on a "need to know" basis. Indeed, although normally a client is the client of the agency rather than of a particular youth care worker, there may be circumstances in which a child entrusts a particular youth worker with

information on the understanding that this is not discussed with others. Under a recent legal provision, the information can in such circumstances nevertheless be passed on if a new youth worker takes over from the first one, or if it is necessary to involve a colleague to assess whether there is a danger to the child. Most fundamentally, however, social care and youth care workers are subject to a strict duty of confidentiality in their work.

Disclosing Data on Demand

The above concerned the question of when a youth care worker can disclose information to other agencies, and to the police and the prosecuting authorities, of his or her own (or the agency's) own motion. The brochure also deals with the question of how such care workers should respond to demands for information from others including, in particular, the police in the investigation of crime.[258]

The basis position is that the general right of the police to demand information to help them in their inquiries into possible criminal offences is subject to the overriding requirements about the protection of "social data", discussed earlier. The relevant provision in the Criminal Procedure Code, § 161 StPO, therefore neither entitles not requires the youth care agency to pass on information to the police, on request. However, there are exceptions.

The main one is that (as we have already seen) the Law on Social Work itself allows the passing on of information by the youth care agencies to the police, as long as this does not harm the provision of assistance to the young client involved. If from this perspective information can be passed on, it therefore must be passed on if the police asks for it. However, the judgement as to whether or not this will harm the youth care agency's work remains left to the agency itself.

The agency is similarly authorised to pass on information to the courts "in relation to judicial proceedings", including criminal proceedings. This can cover the passing on of information to the police, if such proceedings are pending and likely, e.g. when a charge has already been brought. Other provisions authorise the passing on of information from the general youth care agency to the specialised court youth service (comparable to the youth probation service in the UK), and to the family or youth courts in connection with care or custody proceedings. In all these cases, however, there is always the test that this should not harm the provision of help to the child. In serious criminal cases against young persons, the court can order the youth care agency to provide of information – but even it cannot order the production of entire youth care files or the disclosure of particularly "entrusted" or particularly sensitive information.[259] In practice, the court will usually rely on the specialised court youth care service. In principle, the court service

[258] Note that, in Germany, the police investigate criminal offences under the direction of the prosecuting authorities (the *Staatsanwaltschaft*). To avoid confusion in the mind of readers used to the English system, we usually refer to demands for information from the police where the brochure speaks of demands from the prosecuting authorities.

[259] Courts do not have this power in minor criminal cases. Note also again that the age of criminal responsibility in Germany is 14, and children under that age can therefore not be prosecuted at all.

should seek to obtain the data from the young person him or herself, but in certain cases the ordinary youth care agencies can pass on information to this specialised service – again provided that this does not harm the support provided to the young person.

Other Agencies or Persons Passing On Data to the Youth Care Agency

Private-sector institutions such as private kindergartens, schools and private drug clinics etc, are subject to the more relaxed data protection rules relating to that sector, contained in the Federal Data Protection Law. These generally allow the passing on of non-sensitive information to the state youth care agency if this is, on balance, in the interest of a child or young person, and of sensitive data if this is necessary to prevent harm. However, some professionals in the private sector are subject to special duties of confidentiality, and then their freedom to disclose data may be more limited. Doctors, psychiatrists, etc. can only pass on information to the youth care agency (or, for that matter, to the police) with the consent of the patient (and/or, if this is a child, his or her parents) or if there is an immediate emergency threatening serious harm. As earlier noted, the police is furthermore given special powers to pass on information on young people involved in crime to the youth care agencies, as a means to assist in de-criminalisation.

A.4 Conclusions

We hope that the above makes clear the restrictive approach to data sharing in Germany, which however still allows for the passing on of information on children, on the basis of very carefully phrased legal rules. The main overall principles are:

- that professionals involved in youth care are under a very heavy duty of confidentiality in respect of any personal data they collect on their young clients, and especially in respect of any data that are "entrusted" to them (i.e. that are provided to them in a relationship of trust);

- that any obtaining of data by any public body, any disclosure of data by any public body to another public body, and any receiving and further use of the data by the other public body, requires a specific legal basis; and that the confidentiality rules relating to "social data" entrusted to youth care workers and teachers override more general rules allowing other bodies – including the police – to request or even demand information (which is almost the opposite of the legal position in the UK);

- that this does not prevent disclosures of personal data on children and young persons if this is necessary to protect them from harm, or if the disclosure does not undermine the providing of assistance to the children and young persons concerned;

  but crucially:

- that the decision on whether to disclose data on a child or young person is ultimately always left to the youth care professional: s/he should decide to disclose or not to disclose data on the sole basis of what is in the best interest of the child.

Consequently, because this must always be a case-by-case decision:

- that there can never be arrangements which require the disclosure, in "joint" or "on-line" arrangements of any "entrusted" (confidential) data without due consideration of the individual case; and *a fortiori* no completely interlinked databases in which basically all data from different agencies dealing with children and young people are open to all.

These strict principles derive partly from respect for data protection principles, but are reinforced by a tradition of decentralisation of power and, perhaps most importantly, by recognition of professional expertise and the need to allow professionals to exercise professional judgement and discretion in the performance of their job. Yet in Germany, too, these principles are under threat from attempts to centralise, control and take away such freedom of action from the professional (youth) carer.

(B) The Legal and Regulatory Framework in France [260]

B.1 Background

France was one of the first countries in Europe – indeed in the world – to adopt a national data protection law, the Law on Informatics, Files and Freedoms of 1978.[261] The Law was substantially amended in 2004 to bring it into line with the EC Framework directive on data protection,[262] but the basic principles underpinning the Law, the basic regulatory approach, and the basic approach of the French data protection authority, the National Commission for Informatics and Freedoms or CNIL,[263] have remained the same. As will be shown below, some rulings and decisions dating back to the 1980s are still directly relevant to the subject of this report today.

The main consideration underpinning the Law is set out in Article 1 of the Law as follows:

> *Informatics must be at the service of each citizen. … It may violate neither human identity, nor human rights, nor private life, nor individual or public liberties.*[264]

Data protection is therefore, in France as in Germany, explicitly linked to fundamental rights. However, the link is somewhat different. In Germany, data protection is derived from the (proto) "*right to [respect for one's] personality*" and thus very much a personal right, while in France, as is clear from the article in the law, just quoted, data protection is seen more as a state measure to protect fundamental rights generally against a perceived danger that informatics may fail to "serve mankind". One particular expression of this is the rule that no judicial decision or other decision with legal effect may be taken on the sole basis of "*processing of personal data aimed at creating a profile of the data subject or at evaluating certain aspects of his personality*." (Art. 10 of the current 2004 version of the Law, repeating Art. 2 of the original 1978 Law).[265]

---

[260] This section draws heavily on information kindly provided by Mme. Marie Georges, Mme. Leslie Basse and M. Norbert Fort of the French data protection authority, the CNIL.

[261] *Loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.*

[262] By means of the *Loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel du 6 août 2004*. The full title of the current law is therefore *Loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (modifié par la loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel du 6 août 2004).*

[263] *Commission Nationale de l'Informatique et des Libertés*, herafter referred to as "the CNIL" or "the Commission".

[264] The sentence omitted from the quote adds that "*[informatics] must be developed within the framework of international co-operation.*"

[265] This prohibition in the French Law was the basis for the corresponding prohibition in the EC Framework Directive on data protection, which is now also included in the UK DPA98 (although it has never yet been applied in the UK). On the application of this principle in France, in a context directly relevant to the present study, see below, at 8B.2, under the heading "*The 1981 GAMIN system*".

This has implications for the regulatory approach to data protection. In particular, the French authorities place much less reliance on "*informational self-determination*" – on the contrary, they are very wary of allowing processing simply on the basis of "consent". More generally, where the Germans tend to deduce specific requirements relating to specific processing operations from basic (constitutional) legal principles, the French tend to take a more administrative-regulatory approach, in that they seek to lay down (at least for the public and semi-public sectors) detailed rules setting out the data protection requirements for each specific context. Under the Law, processing of personal data in the public sector must generally either be specifically regulated by a decree adopted after the opinion (*avis*) of the CNIL was obtained, or authorised by the CNIL itself. Alternatively, controllers can – and often will – choose to process data in accordance with general "simplified norms" (*normes simplifiées*), issued by the CNIL for a particular sector or field of activity. In practice, it is rare for the detailed recommendations of the CNIL, as set out in an *avis*, not to be reflected in the decree in question; and the CNIL will also generally not accept departures from the "simplified norms" unless there is a good reason to do so. The regulatory acts concerned (*avis*, *authorisation* or *norme simplifiée*) are thus at the heart of data protection in France. They specify in detail the specific purpose of the processing covered by the regulatory act, the categories of data concerned, the categories of recipients, who may have access to the data, any restrictions on rights of data subjects, etc., etc.

In spite of this somewhat different approach, the overall effect is therefore quite similar to Germany: under the Law, detailed, strict rules are set for the processing of personal data for public purposes in specific, narrowly-defined contexts. The differences tend to lie in nuances.

The CNIL thus plays a central role, not just in monitoring compliance with data protection rules and principles laid down by the legislator, but by playing a strong role in the formulation of those rules themselves. It has a strong reputation as a forceful regulator, and also does not hesitate to play a dominant part in political discussions relating to matters within its competence.

A further matter of importance to the present study is the strong emphasis given, in France, to the duty to maintain "professional secrecy" (*le secret professionel*). If anything, the legal duty not to disclose information held in a professional capacity is more strongly emphasised in law than are data protection principles against disclosures of personal information.

Finally, as concerns minors of school age, it is important to note the basic principle that "education overrides repression", i.e. that the best (educational) interests of the child should always be the primary concern, and that other public interests (such as prevention or detection of crime) are subsidiary to this when matters relating to an individual child are concerned.

Between them, the latter two principles – professional secrecy and the primacy of the interests of the child – tend to strongly emphasise the need for professional discretion:

only the professional dealing with a child can decide whether confidentiality can be set aside in an individual case. Such professional discretion should never be displaced, or undermined, by computers.

B.2 Applying Data Protection Principles in Practice to Data on Minors

In this section, we will first briefly describe the general approach to the collecting and use of personal data on children, developed by the CNIL, including the question of involving parents in the collecting of data on minors at school. After that, we will describe an important case, dating back to the early 1980s but still central to the issues addressed in the project for which this paper is written. This is followed by an outline of the rules (issued in the 1990s) relating to the national student database, and a brief discussion of some other, more recent issues.

The General Approach to Collecting and Use of Personal Data on Minors

In a 2001 report on The Internet and the collection of personal data from minors,[266] the CNIL discussed certain matters not specifically related to the Internet but important to the question of data protection and minors generally, including: the nature of a child, the different ages at which young people are competent to take certain decisions in different contexts, the importance of families and parents, and the Commission's general approach to the collecting of data from minors, in particular also (with reference to earlier decisions) at schools.

On the first point, the Commission quoted a child psychologist, Henri Wallon, describing a child's evolution as follows:

> *A child can only live his youth ... from step to step created by it ... in the succession of its phases; it is a single person yet in transition through a series of metamorphoses.*[267]

Because of a child's lack of psychological, intellectual and physical maturity – because it is still going through these "metamorphoses" – it is considered in law to be in need of special protection against third parties and against negative decisions it itself may take. Consequently, the CNIL stresses that "*the guarantees provided to anyone by [the French data protection law] must be applied with special force as concerns minors*".[268]

---

[266] *Internet et la collecte de données personnelles auprès des mineurs*, report prepared by Mme Cécile Alvergnat (member of the CNIL) and adopted on 12 June 2001.

[267] *L'enfant ne sait que vivre son enfance (...) d'étapes en étapes il se construit (...) dans la succession de ces âges, il est un seul et même être en cours de métamorphoses.* cf. the statement by the German Constitutional Court that a child is a personality "in development".

[268] *Internet et la collecte de données personnelles auprès des mineurs*, op. cit., p. 31, repeated in: *Internet, les jeunes et la protection des données personnelles et de la vie privée*, CNIL Fiche de Synthèse (summary), 19 January 2005, p. 1.

That does not mean that one should not distinguish between children and young persons of different ages and capacities, either in relation to data protection or other matters. Thus, the report points out that the formal legal age of majority is 18, but that this of course does not mean that children and young people under that age are not invested with rights and obligations; and that the law gives certain rights to children of different ages: At 12, a child can obtain a bank (ATM) card (with the consent of its parents); at 13, s/he must consent to a name change or to his or her adoption, and must be heard by a judge in divorce cases; at 15 girls may marry with the consent of at least one parent (for boys, the age is 18, except for special cases); 15 is also the age at which young persons can engage in sexual activity without criminal responsibility, and from which girls can obtain the "morning after pill" and obtain an abortion without the involvement of their parents (if they don't want such involvement), provided they involve another adult;[269] at 16, they can enter into a contract of employment (provided the parents don't object) and can join a trade union, apply for French nationality, and make a will (for up to half of their possessions). Children under the age of 13 are not criminally liable; children between 13 and 16 may only be held in pre-trial detention in exceptional cases of serious crime (*crimes*). There are also special rules on film categories and on marketing to children of different ages. All in all, these various rules show that the legislator accepts that there is no one single cut-off point, but rather, that different criteria should be applied in different contexts.

In this, the child should also not be seen as an individual in isolation. Specifically, the CNIL refers to the preamble of the UN Convention on the Rights of the Child, which stresses that:

> *The family, as the fundamental group of society and the natural environment for the growth and well-being of all its members and particularly children, should be afforded the necessary protection and assistance so that it can fully assume its responsibilities within the community.*

In various contexts, the Commission therefore strongly emphasises the need to involve parents in matters (including data protection matters) relating to young people.

Thus, already in 1983, the CNIL ruled on the collection of personal data from children in schools. The case arose out of a complaint concerning the handing out of a questionnaire to (under-age) students in a secondary school (*collège*). The CNIL ruled that the questionnaire should not have been given to the students without the **prior written consent** of the parents.

In 1985, it adopted a general recommendation on the collection of personal information in schools (*en milieu scolaire*). The recommendation (which is still in force) covers all questionnaires used in school establishments: forms filled in by students for teachers, files on registered students and applicant students, feedback forms (*enquêtes*), etc.; and addresses in a general way all collection of information on school children or their

[269] At the time of the report (2001), this was still a legislative proposal, but it has since become law.

families. In it, the CNIL says that under-age students may not be subjected to psycho-technical or psychological tests or assessments (*à des tests ou épreuves à caractère psychotechnique or psychologique*) without "*the written agreement of the person [asking the youth to take the test?], in which the latter accepts legal responsibility*" (*l'accord écrit de la personne qui en assure la responsabilité légale*). In other words, any person (or school etc.) carrying out such a test must warrant that the test is legal. This is a double test: the person (school etc.) concerned must be legally permitted to carry out such a test, and the details of the test must be in accordance with the law (including of course, in particular, the Data Protection Law).

Since then, the CNIL has required the prior written consent of parents for the dissemination of photographs of minors on the Internet (e.g. on a school website) and for the passing on of contact data on minors for the purposes of direct marketing.

On the issue of children and the Internet (with which the report from which the above general considerations were taken was specifically concerned), the CNIL ruled, *inter alia*:

- that the principle of purpose-specification and limitation should be particularly strictly applied as concerns the collection of data from minors;

- that all collecting of data from minors on their family circumstances, their parents' lifestyle and their social and professional status must be considered as *ipso facto* "excessive and unfair"; and

- that the recording of data relating to racial origin or to political, philosophical or religious opinions, trade union membership or the morals of all individuals without their consent is (in principle) prohibited by the law; and that the collecting of such data from children is therefore also prohibited, unless the controller can provide proof that the parents have expressly consented to this.[270]

While set out in the particular context of the Internet, and more specifically to data collecting by private-sector bodies over the Internet, these principles should also be borne in mind in relation to the collecting of data on children in other contexts. Put simply, while there may be special justification for the collecting of data on children in the public sector, this too should be subject to strict purpose-specification and limitation; parents should be fully informed and in principle asked for their (written) consent; data on siblings and parents should not be obtained from children;[271] and the collecting and further use (and of course especially the disclosure) of sensitive data on children should be particularly strictly circumscribed, in rules drawn up by, or drafted following the advice of, the CNIL.

---

[270] *Internet et la collecte de données personnelles auprès des mineurs*, op. cit., pp.31-32. The report adds that parental consent is also necessary for the passing on of data on minors in connection with the playing of games or the holding of lotteries etc. on the Internet.

[271] While not as formally stipulated as in Germany, France too adheres to the principle that whenever possible personal data should be obtained directly from the data subject, rather than indirectly, from others, in that collection from others will often be regarded as "unfair" and thus contrary to the Law.

The 1981 GAMIN System

Of particular importance to the present study is a decision by the CNIL of some 25 years ago, concerning the proposed establishment of an automated system aimed at identifying families and children in need of special attention from the social services.[272] Compared to the data-sharing arrangements being put in place in the UK at present, the French proposals of the time seem modest and subject to significant restrictions. However, the CNIL nevertheless issued a negative opinion (the first ever negative opinion issued under the 1978 Law) and thus prevented the system from becoming established.[273] It is therefore worthwhile to examine this case in some detail, especially since the CNIL still takes the same view of such matters.

The project – called "GAMIN" (French for 'brat' or 'urchin') – was intended to involve the automated processing (and analysis) of data from the health certificates which by law have to be drawn up by a doctor on any new-born child and its mother, and of other data to be obtained from the family.

The purposes of the planned system were to be:

- to allow for a better targeting of the actions of Mother and Child Protection Teams (MCPTs) to families most in need of their assistance;

- to help the MCPTs ensure that children suffering from a disability or affliction [*un handicap ou une affection*] received the necessary assistance;

- to provide the Ministry [of Health] and the State with anonymised statistical information on the state of health of young children as a means towards improving the MCP service to the population at large; and

- to contribute to medical research, in particular by improving the etiology of disabilities and afflictions and putting in place effective mechanisms of prevention.

The medical data were to be obtained from the doctor who issued the relevant certificates; and the other data from the families concerned. (The only other data to be processed in the system would be administrative data needed for the processing). The computer system was to remain based in (or at least under the control of) the Ministry of Health, and the medical doctor of the MCP service was to retain sole control over any

[272] Although the system was reported to the CNIL as merely a project, it was in fact implemented in 34 *départements* (administrative regions) pending the opinion of the CNIL.

[273] *Déliberation No. 81-74 du 16 juin 1981 portant décision et avis relatifs àun traitement d'informations nominatives concernant le traitement automatisé des certificats de santé dans les services de la protection maternelle et infantile.* The opinion is in the rather formal "considering that" style. In the quotes in the text, we have revised this to more easily-comprehensible direct language. The translations are also somewhat free, to give the sense of the CNIL's considerations. The CNIL gave the 34 regions one year to dismantle the system.

disclosures of the data. He would have been under no hierarchical authority in this respect.

If the system had been established, the doctor could have used it to decide to disclose "*certain indications*" (read: of a need to intervene) to the MCP's socio-medical teams, for the sole purpose of protecting mother and child. Data could only be passed on to persons or services outside the MCP service if the recipients were also subject to the duty to maintain medical secrecy (an especially high kind of professional secrecy). The data were not to be linked to or systematically joined with other automated databases.

The CNIL felt that, in spite of these safeguards, it still had to closely examine the compatibility of the proposed system with the Law. After "numerous discussions", it accepted that a "flag of concern" about a child (*fiche de signalement d'enfant prioritaires* or FEP) was not, in itself, a "profile" in the sense of what was then Art. 2 of the Law (now Art. 10) – which, as we have seen, prohibits the taking of "decisions with legal effect" on the basis of such "evaluations". The CNIL accepted that the "flag" was just an aid to decision-making (*un élément d'aide à la décision*) by the doctor, who also had other "preventive tools" at his disposal, and that the "flag" (the FEP) therefore did not constitute the "sole" basis for the subsequent decisions on the child to which it related.[274]

However, the CNIL still found that:

> *"the main purpose [of the GAMIN system] is the pre-selection, by automated means, of children who, according to the computer programme [selon la logique du système], should or should not be the object of medical and social assistance."*

The selection or non-selection was based on a computerised model assessing medical-social risk factors calculated on the basis of some 170 items of information. However, according to the CNIL:

> *"Such computer-modelling, even if it allows for the establishment of mostly relevant presumptions about the situation of children, in itself contains uncertainties that cannot be corrected by subsequent checks, on a case by case basis, of the MCP doctor ... many practitioners oppose such a practice as inadequate [for its purpose].*
>
> *[Furthermore,] excessive reliance on such a process could lead to missing out non-selected children, even though some of them may need special help, and to the setting of priorities of means and of assistance on the basis of a dubious form of determinism [un déterminisme contestable].*
> ...
> *There is [also] no medical consensus on the criteria to be used to detect and identify [children and families in need], that can be derived from the [medical]*

[274] This is important because if a computer-generated "signal" or "flag" were to form the sole basis for a decision by a public authority to intervene with a family, this would contravene Art. 10 of the Law (Art. 2 Old) and would thus always be unlawful.

certificates and [usefully] processed by computer to this end: the number of criteria usually said to be kept in the so-called national indication table [table de signalement] is much lower than the number of criteria in the health certificates.

There are regional variations resulting from the fact that these matters are left to the MCP doctor and [depend on] the means at his disposal.

The system is also heterogeneous in that the criteria are different in nature: some are objective, i.e. they record a fact, while others depend on the [subjective] assessment of the doctor.

Some of the criteria are taken directly from the medical certificates and are pre-defined by them, while other criteria (so-called 'generated criteria' [critères dits générés]) are the result of combinations of different data.

Administrative data, social data and socio-professional data are used together with purely medical data.

The structural weakness of the system is aggravated by other factors, such as the qualitative and quantitative differences in details recorded by the doctors in the medical certificates, or in the retention periods for data held by doctors and MCP teams for the purpose of taking decisions on medical and social checks on young children irrespective of the creation of an 'at risk flag'.

The system ... therefore appears to be either dubious, or useless or unusable for it main purpose [soit contestable, soit inutile ou inutilisé]."

The pre-selection, by computer, of children for the purpose of subjecting them to medical or social supervision – which was a particularly sensitive area, as was clearly from the concern expressed by several parental and trade-union associations – therefore raised objections of principle, relating to the very spirit of the Law, as set out in its first article (which, as we have seen, stresses the need for informatics to be at the service of mankind and not to violate basic human rights). The CNIL therefore opposed the establishment of the system (except insofar as it allowed the use of anonymous data for statistical and research purposes).

The CNIL subsequently approved a more limited, experimental system for ten departments for three years which allowed the creation of two separate files (without links) and the disclosure of limited information from the medical certificates to the social services in certain circumstances – but notably without the use of any computer-generated "flags of concern". Indeed, all existing GAMIN systems, and all previously created "flags" of that kind, had to be destroyed.[275]

[275] *Déliberation No. 83-24 du 15 mars 1983 portant avis sur les traitements automatisés relatifs aux certificats de santé du jeune enfant.*

It is clear from the above that, in France, computer-generated "alerts", identifying children (or, for that matter, anyone) as in need of special attention by social services etc. on the basis of heterogeneous, difficult-to-verify or difficult-to-challenge data, are seen as violating the most basic principles underpinning data protection: that "human identity" should never be reduced to a formula, a computer model, and that no significant decisions should ever be reached in this way. This even holds true if it involves computer analysis of data held by just one agency. Notable is also the objection that over-reliance on such a system would let others who are not "flagged" fall through the net. The idea that data from different agencies, obtained for different purposes, can be joined in such an endeavour is, in France, quite unthinkable: it would aggravate an already unacceptable proposition. Most importantly, these principles have not changed since the 1980s: they are still held sacred today.

The 1995 National Student Database (SCOLARITÉ)

In 1986, the CNIL issued a "simplified norm" (Simplified Norm No. 29) on "automated personal data processing systems relating to the general, financial and educational administration of schools and establishments of secondary education in the public and private sector".[276] This was followed, in 1995, by a set of rules issued by the Ministry of Education "on the establishment of an automated personal data processing system for the monitoring/evaluation (*pilotage*) and administration of secondary and academy school students": the "Scolarité" system.[277] The ministerial rules (hereafter: the Rules) apply to all processing subject to Simplified Norm No. 29 (Article 9 of the Rules).

The aim of the system is to allow the general, educational and financial administration of students in secondary schools, the monitoring/evaluation, administration and inspection of academies (which provide adult education), and the monitoring/evaluation of some of the students involved at national level (Article 1).

The Rules allow for the holding of data on students at state secondary schools and academies, and for the disclosure of most of those data to the ministry; private schools can join the system if they wish (Articles 2 and 3).[278] It should be noted that this includes data on part-time students who are also part-time employed, and data on adult students (in particular, at academies). Students cannot "opt out" of the system: their ordinary "right to object to processing" does not apply to the "Scolarité" database (Article 4). The data may only be used within the educational establishments and within the Ministry

[276] *Délibération n° 86-115 du 2 décembre 1986 concernant les traitements automatisés d'informations nominatives relatifs à la gestion administrative, comptable et pédagogique des écoles et des établissements d'enseignement secondaire du secteur public et privé (Norme Simplifiée No. 29).*

[277] *Arrêté du 22 septembre 1995 portant création d'un traitement automatisé d'informations nominatives relatif au pilotage et à la gestion des élèves du second degré portant sur les trois niveaux : établissement, académique, administration centrale*. Both sets of rules have been amended several times: the Rules in 1997, 1998 and 1999; the Simplified Norm most recently in 2004.

[278] The discussion here will be limited to the rules for State schools. It may be noted however that the lists of data and of recipients, discussed in the text, were augmented in 1998 in particular, to allow for the central recording of information on state scholarships for students in private *collèges*.

(Article 5, first sentence): the data are not disclosed to any other agencies or services of the French Republic. They are retained for no longer than two years (Article 6).

Article 5 of the rules specifies exactly what data are to be held by schools and academies, and centrally, as follows:

The following basic student data may be recorded by a school and used for the school's own internal general, educational and financial administration: name, first name, gender, date of birth, place of birth, whether the student is an adult or not and whether s/he is an orphan, national student number or provisional student number, number of the school in question, student's own address and telephone number (if s/he is an adult), or the addresss and telephone number of his/her parents or legal guardians (if s/he is a minor) and also, in the latter case, their name, the number of children in the family, relationship with the guardian, and whether the parents/guardians gave permission for their contact details to be disseminated (e.g., in a students address list), and [other] contact persons and details (such as the contact details of the personnel office of an employer of a part-time student). The system also records the "socio-professional status of the father and/or of the mother", and the student's nationality – but the information on nationality may only be used for statistical purposes. The system furthermore contains information on the student's current school/academy year, such as the course and options taken, and on the previous year including, where appropriate, details of any previous educational institution or employment; information on scholarships, grants and bank details, etc.; and details of requested work placements (*voeux d'affectation*).

In some administrative regions which only became part of France after the Second World War (i.e. the départements of Haut-Rhin, Bas-Rhin and la Moselle) religious education is provided as an option in State secondary schools, and in those regions a record is also kept of whether this option is taken up.

Largely the same information is kept by the academies, but since no religious education is provided there, even in the regions just mentioned, no record of that kind is retained. Also, since students at the academies are adults, there is no need for a record of whether they are minors or adults. However, the identity of any legal guardian is recorded, and the relationship they have with the student. The system still also records the "socio-professional status of the father and/or of the mother".

At the national level, apart from the special case of "student sample groups" noted below, only data on students following a higher-level (post-baccalaureate) course are registered. The data are basically the same as for the academies (i.e. like the data for schools but minus the categories just mentioned), but the data do not include the names of students, or information on the specific town (*commune*) where they were born; rather, it includes only information on the region (*département*) where they were born. The data are nevertheless still regarded as personal data (and thus subject to the 1978 Law) because they include the students' national student number. The aim is to allow detailed

monitoring of students' educational progress etc. by the Ministry, but without the information being used directly in relation to any particular student.[279]

Provision is also made for the keeping, at the national level, of data on "students sample groups" (*panels d'élèves*), made up of a sample of no more than 5% of students on whom data are collected by means of a questionnaire, so as to monitor what happens to them after they leave education. The rules do not specify how the sample is selected, or clarify whether the selected students are asked to consent to this use of their data. The data are the same as the data held by academies, as noted above.

The rules go on, in Article 7, to specify to which officials or bodies the data can be sent, "within the limit of their respective functions" – i.e., the officials and bodies listed can only ever be sent such of the data listed earlier as are needed by them to fulfil their functions (as defined by law).

Schools can give access to the data to their administrative and teaching and educational support staff, to the local mayor (who is responsible for checking that children of compulsory schooling age actually attend school), and to careers advice staff. However, these rules are subject to the proviso just mentioned, and the general requirement of "necessity" in the Law. Thus, the janitor cannot be given access to financial information on pupils, and the mayor need only be provided with information on whether a child attends school, rather than detailed exam results. In other respects, the rules themselves provide restrictions. Thus, parents' associations can be provided with the addresses of students, if (and only if) the parents agreed to the disclosure of this information; they are not to be given any other information on students. An amendment in 1997 adds to the list of recipients, the offices paying out child support payments to families with children aged 16–18 in full-time education. Here, the amendment specifies that these offices can be provided with the following data (only): name, first name, date of birth of the student, name and first name of one of the parents, and place of residence. A further amendment in 1998 allowed the disclosure of data to the local authority offices paying support for a return to school; here, the data are limited to name and first name of the student, name and first name of the legal guardian, and the amount of money paid to the student.

Academies can provide the data they hold to their administrative staff, to academy inspectors, and to their statistical service. But this is again subject to the limitations just mentioned. The statistical service does not need, and therefore should not be provided with, the data in fully identifiable form: information in anonymous or pseudonymous form (in the latter case, e.g., in the form of data linked only to the student number) will suffice.[280] Under another 1998 amendment, they can also provide the data they hold to academy inspectors, in relation to the provision of State scholarships for studying in a private school.

---

[279] The clause allowing academies to process data on nationality in this case does not explicitly restrict the use of such data to statistical analysis only. However, that is possibly implicitly assured.

[280] cf. *Décret n° 84-628 du 17 juillet 1984 relatif au Conseil national de l'information statistique et portant application de la loi n° 51-771 du 7 juin 1951 modifiée sur l'obligation, la coordination et le secret en matière statistique.*

The data held by schools and academies can only be provided to the central (national) authorities for the purposes of evaluation and forecasting. This means that they can only be provided in anonymous or pseudonymous form, and that they must be processed in accordance with the (strict) rules on the processing of personal data for statistical purposes: these stipulate, in particular, that data that are processed for such purposes may never be used in relation to (and in particular not to take decisions on) the data subjects.

Finally, the Rules allow for the disclosure of the data held on students to the students' parents.

The Simplified Norm and the Rules thus strictly limit the amount and nature of the data that are kept by educational establishments, and restrict even more the disclosure of those data, especially to the central authorities (the Ministry for Education). Specifically:

> *"Other personal information may not be disclosed to other third parties without the written consent of the student him/herself if s/he is legally competent, or his/her legal guardian, unless otherwise provided by law."* (Article 5, last sub-clause, of Simplified Norm No. 29) [281]

The point to be made about this last stipulation is that the "contrary legal provision" referred to must be a specific one: under French constitutional law and data protection law, one cannot invoke a general catch-all provision as authorising a disclosure: broadly-phrased provisions (which of course can be found in various laws) cannot constitute specific "contrary legal provisions" of the kind referred to. This is because data protection is seen as a fundamental right, and disclosures of personal data as interferences with a data subject's rights, which require a clear and specific legal basis. An example of a specific provision would be, for instance, a provision allowing tax inspectors investigating benefit fraud to ascertain whether a family receiving financial support for children in full-time education were really entitled to such support (i.e. to ascertain whether the children in question were actually enrolled in such education).

There are no specific provisions allowing disclosure of data on students in order to generally identify (through computer analysis or otherwise) whether any of them are likely to need special attention by social or child protection services. As should be clear from our earlier comments about the GAMIN system, the CNIL would strongly oppose the adoption of any such specific provisions – and the Commission would, in the French system, be extensively consulted on the drawing up of any such rules. The idea that, in the absence of specific provisions, general catch-all provisions would suffice, is, in France, quite unthinkable.

[281] *Sauf disposition légale contraire, toute autre information nominative ne peut être communiquée à des tiers qu'avec l'accord écrit de l'élève lui-même, lorsque celui-ci en a la capacité, ou de son responsable légal.*

Recent Cases: Geo-tracking of Children; Biometrics in the School Canteen

Since the 2001 report on the Internet and children, discussed earlier, the CNIL has addressed a number of further data protection issues relating to children, which should be briefly mentioned.

In 2003, the CNIL was asked for its views on a service being offered in France (as now also in the UK), which allows people to check the place where a particular mobile telephone handset might be. The service is aimed in particular at parents wanting to keep track of the whereabouts of their children.[282] The CNIL noted that the Directive on Privacy and Electronic Communications (Directive 2002/58/EC) – which is subsidiary to the Framework Directive (Directive 95/46/EC) – requires the consent of subscribers for such a service, but does not clarify the question as to who should give this consent in relation to minors. The Commission did recall however that it had ruled that the rules set out in these directives should be particularly strictly applied to geo-tracking services generally, and that it therefore requires, first of all, that the subscriber gives a positive reply, by SMS, to a message confirming that the service has been taken up, and subsequently, that an SMS is also sent to the mobile phone every time the phone's location is checked, informing the user of this fact and of the identity of the person asking for the check.

On the use of this service to keep track of children, the Commission did not provide definitive answers. Rather, it conducted an Internet poll, seeking the views of parents and children, and on that basis set out the issues from different points of view. From the parents' point of view, the service provided reassurance in a challenging world, in which children often roamed freely. They often saw the service as a kind of "contract" within the family: greater freedom for the child in exchange for a new means for parents to know where they were. In this sense, the service was a response to a modern "need".

However, children also have rights, as defined in particular in the UN Convention on the Rights of the Child. Indeed, the Convention stipulates, in Article 3, that:

> *In all actions concerning children, whether undertaken by public or private social welfare institutions, courts of law, administrative authorities or legislative bodies, the best interests of the child shall be a primary consideration*

Is it, the Commission asked, in the best (higher) interest of the child that its parents can determine where it is at any given moment? Indeed, is that legitimate?[283] In an earlier case, the Commission had held that "web-casting" pictures from a crèche on a webpage intruded too much into the private life of the (very) young children in question. If that

[282] CNIL, Annual Report 2003, pp. 140 – 142. See also the page with results of the Internet poll on the CNIL website: www.cnil.fr/index.php?id=1557.

[283] Note the use here of the term "legitimate" in a much wider sense than "lawful": see the discussion in Chapter 7 of the terminology used in the DPA98.

was so for a young child in a crèche, was it not also the case for a child or adolescent old enough to use a mobile phone?

More specifically, the Commission wonders if the use of such a service doesn't "upset the normal interplay of trust between parents and children":

> *"Doesn't this service, in a perverse way, tend to favour a disengagement of parents who may get the illusion of being in charge of – or at any of being able to check – the activity of their children?"*

And finally:

> *"From a societal point of view, doesn't the development of such services tend to getting individuals used, from an early age, to a form of semi-permanent surveillance, so that he is not even any longer aware of the intrusiveness of such measures?"*

The responses to the Commission's Internet poll did not provide clear answers to these questions. Parents in favour of the system stressed the perceived benefits in terms of more security for their children. However, they seemed to confuse their own powers to know where their children were with the possibilities of the police to take action to find people. They stressed that they would use the system reasonably – but at the same time expressed the strong view that by knowing where their child was, they would also know what the child was up to! (The Commission added an exclamation mark to this finding, as if to underline that geo-location information in fact reveals more than just the geographical position of the mobile 'phone user.) Respondents who were against the system pointed to the dangers (also noted by the Commission) of slipping into a surveillance society, of undermining the necessary autonomy of young people, and of parents abdicating their responsibilities to machines.

The CNIL decided to continue to study the issue. In the meantime, it is clear however from the Commission's own critical comments that it has great doubts about the "legitimacy" of the system. More generally, and more directly relevant to the present study, it is clear that the Commission lays great score by the need to allow young people their own space, and is fearful of a society in which technology is used to ever-increase surveillance over the actions of youngsters and adults alike.

The same is clear from the CNIL's stand on the use of biometrics, and of hand-contour readers in particular. In 2005, the Commission approved a range of uses of such readers, because the systems were configured in such a way as to allow verification of the identity of the person without this leaving any traces: [284]

[284] *La reconnaissance du contour de la main: une technique biométrique qui ne laisse pas de traces*: CNIL, 29/07/2005, last amended on 25/10/05, on http://www.cnil.fr/index.php?id=1853.

> *"No image or photograph of the hand is retained. Only a biometric key (a string of characters), generated by means of an algorithm, creates a link to the identity of the person."*

Specifically, if (on the basis of this algorithm) the system grants access to certain places, that is all the approved system does: it does not keep a record of having granted this person such access at a particular time:

> *"Notably different from finger prints, a hand contour effectively consists of biometric data that do not leave traces that can be used for purposes other than the purposes defined by the controller."*

The use of such a system is therefore, in the light of current technologies, an unacceptable system under the 1978 Law, whereas using fingerprints and retained data would not be.

Because of this, the CNIL authorised the use of hand contour technology in a number of schools, to control access to the canteen by pupils.[285] However, even for the schools authorised to use hand-contour technology, the CNIL ordered that the legal guardians of the pupils should be individually informed of the new system, and that they should be given the opportunity to refuse to allow the use of biometric data on their children – even for the approved (non-trace-leaving) systems. The schools should therefore provide for an alternative means of allowing access to the canteen for those children whose parents objected to the hand-contour access system.

By contrast, the CNIL refused permission for the use of (trace-leaving) digital fingerprints in other contexts, such as work places. It ruled quite generally that access-control systems do not generally require retention of data on when access is granted to whom, and that systems aimed at checking whether people were at their place of work also do not need the storing of access data. Using trace-leaving systems for these purposes, where the non-trace-leaving technology of hand contours would serve, would be neither suited nor proportionate to the purpose to be achieved.

B.3 Conclusions

The French data protection authority, the CNIL – the equivalent of the UK Information Commissioner in matters of data protection – plays a central role, not just in monitoring compliance with data protection rules and principles laid down by the legislator, but also in formulating many of the rules itself; and it plays a dominant part in political discussions relating to matters within its competence.

The CNIL believes that "*the guarantees provided to anyone by [the French data protection law] must be applied with special force as concerns minors*". Put simply, while there may be special justification for the collecting of data on children in the public

[285] *Biométrie: quatre refus d'autorisation d'utilisation des empreintes digitales*: CNIL, 30/01/06, on http://www.cnil.fr/index.php?id=1938&news[uid]=304&cHash=1b5bb06ad5.

sector, this should be subject to strict purpose-specification and limitation (including clear and narrow purpose-definitions); parents should be fully informed and in principle asked for their (written) consent for the processing of data on their children; data on siblings and parents should not be obtained from children; and the collecting and further use (and of course especially the disclosure) of sensitive data on children should be particularly strictly circumscribed, in rules drawn up by, or drafted following the advice of, the CNIL.

The CNIL also insists that parents should be closely involved in data protection matters relating to their children. Thus, questionnaires should not be given to school children without the prior written consent of the parents; and such prior written consent of parents is also required for the dissemination of photographs of minors on the Internet (e.g., on a school website) and for the passing on of contact data on minors for the purposes of direct marketing. Under-aged students should also not be asked to perform psycho-technical or psychological tests or assessments.

It is clear from an early-1980s ruling ("GAMIN") – which would still be followed today – that in France, computer-generated "alerts", identifying children (or, for that matter, anyone) as in need of special attention by social services etc. on the basis of heterogeneous data that are difficult to verify or challenge, are seen as violating the most basic principles underpinning data protection. "Human identity" should never be reduced to a formula, a computer model, and no significant decisions should ever be reached in this way. This even holds true if it involves computer analysis of data held by just one agency. One objection is that over-reliance on such a system would let others who are not "flagged" fall through the net. The idea that data from different agencies, obtained for different purposes, can be joined in such an endeavour is, in France, quite unthinkable: it would aggravate an already unacceptable proposition.

The rules on the system for collecting and storing of personal data on students at secondary schools and academies (the "SCOLARITÉ" system) strictly limit the amount and nature of the data that can be collected by these institutions, the recipients of the data, and the uses that can be made of them. They are particularly strict in the limitations imposed on the uses that can be made of the data by the central (national) authorities. It is clear from these rules (and from the GAMIN-ruling) that the CNIL would strongly oppose the adoption of any specific provisions allowing disclosure of data on students in order to generally identify (through computer analysis or otherwise) whether any of them are likely to need special attention by social services or other child protection bodies. The CNIL would, in any case, be extensively consulted on the drawing up of any such specific rules. The idea that, in the absence of specific provisions, general catch-all provisions would suffice, is, in France, quite unthinkable.

The strict approach to the processing of personal data on minors, and to the use of intrusive technologies in this regard, is also clear from the decisions by the CNIL with regard to the use of biometric data for access to school canteens, and from its (so far, only tentative) comments on the use of geo-location services to track the whereabouts of mobile 'phones used by children.

(C) Selected Issues in Various Countries [286]

Some special issues, relevant to this study, are addressed in some EU Member States in ways that may be of interest to the Information Commissioner in the present context. Two issues stand out as having been addressed in quite a few countries: the question of when national identity numbers and other "general identifiers" can be used, and the related question of when different databases can be linked up (or "interconnected") for the purpose of data sharing. The law and practice on these issues in those countries are briefly summarised in the next two Sections, D.1 and D.2. Section D.3 deals with the special rule the Framework Directive (also contained in the DPA98) on the taking of fully automated decisions. In the final Section (D.4), we will assess these matters with reference to the processing addressed in this study, draw conclusions and make recommendations.

C.1 Processing Involving a National Identification Number or Another "Identifier of General Application" [287]

> *"Member States shall determine the conditions under which a national identification number or any other identifier of general application may be processed."* (Article 8(7) of the EC Framework Directive on data protection)

Not all Member States have national identity numbers, although in several of the ones that don't have general ID numbers yet, the introduction of such numbers is being discussed. It is not inconceivable that the EU will at some stage try to introduce EU-wide identity numbers (or at least an EU-wide database of national numbers, and measures to avoid duplication or conflicts between them). In the UK, such a number will effectively be introduced through the ID cards register. However, as we have seen, there are already numbers in use in the UK which serve as "identifiers of general application": the National Insurance Number and the Child Reference Number (jointly to be used as the basis for the unique identifying number in the ISA), the Unique Pupils Number, the NHS number, etc. The same is true in other countries: national numbers and more specific numbers often coexist. On the Continent and in Ireland, there are different approaches to the use of such numbers, but all involve restrictions on their use.

The law in Finland stipulates that the use of the national identity number is generally allowed with the consent of the data subject, but imposes strict limitations on its use without consent. By contrast, some other countries, including Denmark and the Netherlands, allow for wide uses and exchanges of this number between public bodies,

[286] The information in this section is largely taken from: D Korff, Comparative Study and from the relevant country reports in D Korff, Data Protection Laws in the European Union, updated where possible from the websites of the relevant data protection authorities.

[287] For general background and an overview of the situation 15 years ago, see the Council of Europe report, The introduction and use of personal identification numbers: the data protection issues (1991).

also without consent, if this is useful for the work of the bodies in question. However, this is, in these countries, still always subject to the general "purpose-limitation" principle: the number may not be used to enable disclosures of data (or data sharing) which would contravene that principle. Thus, in The Netherlands, the use of an identifying number issued for a particular purpose (say, for data sharing in the education sector) for a different purpose (say, for social welfare) requires a "prior check" of the kind discussed under the next heading. In Sweden the use of the national number, even with the consent of the data subject, must still be "clearly justified" – which in practice also refers to purpose-limitation.

In Ireland, the so-called Personal Public Service Number or PPSN (which succeeded an earlier number, the Revenue and Social Insurance [RSI] Number) was introduced in 1998 by means of social welfare legislation. This number is used in all dealings with public authorities – but may not be used by private bodies (or indeed asked for by the police). The Data Protection Commissioner has, after consultations, stopped some data exchanges between public authorities on the basis of this number, but remains concerned about the potential for abuse. The Commissioner hoped to issue a code of practice on the use of the number before the end of 2002, but no such code appears to have been issued as yet. He has stressed that he is not opposed to the Public Service Number as such – indeed, would not be opposed to a full national identify number – because he feels that the issue is not the existence or otherwise of such a number but the constraints placed on its use, and the effectiveness of the enforcement of such constraints.

In France, processing of personal data sets which either include the national identity number of the data subjects concerned (the NIR), or which requires consultation of the national database of these numbers (the RNIPP), requires "prior authorisation" from the CNIL, and are strictly controlled, again in particular with reference to purpose-limitation. The CNIL has sought to limit the use of the number to clearly specified circumstances, for clearly defined purposes, and has attempted, in particular, to prevent the use of the number for the creation of (unregulated) interconnections between databases operated by different (mainly public-sector) bodies, for different purposes – contrary to the rules noted in the next sub-section.

In the UK, the Secretary of State can issue an order under para. 4 of Part II of Schedule 1 regulating the use of such numbers – but contrary to the requirements of Article 8(7) of the Framework Directive, set out above, no such order has as yet been issued.

C.2 Restrictions on the Creation of Interconnections Between Different Databases

In practice, as the CNIL (and the Irish Commissioner, and others) have noted, the use of general identifiers is closely linked to the linking – or interconnecting, as it is usually called on the Continent – of different databases, i.e. to data sharing. Indeed, that is often the main purpose of such numbers. The restrictions on the use of such numbers, noted above, are generally aimed at limiting such links, such data sharing. Thus, the stipulation about the need for "clear justification" in Sweden effectively means that the general

number may only be used to facilitate links between different data collections if the disclosures and sharing involved is justified. And, as noted, the "purpose-limitation" principle limits the otherwise seemingly lax rules on the use of general identifiers for data sharing in Denmark and the Netherlands.

Other countries deal with the question of interconnections directly by imposing special procedural restrictions on them, on the basis that such links between different databases inherently pose risks to the rights and freedoms of the data subjects concerned. These restrictions correspond to those envisaged in Article 20 of the EC Framework Directive, which reads as follows:

> *Article 20*
> *Prior checking*
>
> *1. Member States shall determine the processing operations likely to present specific risks to the rights and freedoms of data subjects and shall check that these processing operations are examined prior to the start thereof.*
>
> *2. Such prior checks shall be carried out by the supervisory authority following receipt of a notification from the controller or by the data protection official, who, in cases of doubt, must consult the supervisory authority.*
>
> *3. Member States may also carry out such checks in the context of preparation either of a measure of the national parliament or of a measure based on such a legislative measure, which define the nature of the processing and lay down appropriate safeguards.*

In Austria, Greece, Luxembourg and Portugal, all "interconnections" between files (databases) and all "combinations" of data (data matching, the result of data sharing) require a permit from the Data Protection Authority, or are subject to the requirement of a "prior check" or "prior authorisation".

As we have seen, in France, too, the interconnection, by automated means, of personal data filing systems which are established for different purposes require "prior authorisation" from the CNIL. In principle, this, and the same requirement for the processing of the national identity number, noted earlier, should give the CNIL extensive scope to impose strict limitations. However, it has warned that the convergence of electronic protocols means that data exchanges are becoming easier even without the use of any single, central identifiers; and said that there is therefore a need for a fundamental re-appraisal of the issues. The aim of this re-appraisal would be to further tighten the rules in respect both of the use of general identifiers and of the creation of interconnections they allow.

Thus, in many EU countries, the linking of databases, and/or the use of general identifiers that facilitate such linking, are regarded as posing inherent risks to the rights and

freedoms of data subjects that should be addressed by special, strict substantive and procedural rules.

It may be noted too, that in quite a few countries the processing of sensitive data is required as always, or in certain circumstances, "risky" in the sense of Article 20 of the Directive, and is thus made subject to the requirement of a "prior check" (or "prior authorisation", or a permit). This is the case in Austria, in Finland and Portugal (if it is claimed by the controller that the processing is for a reason pertaining to an "important public interest"), in Greece (even if the processing is with the consent of the data subject), and in Germany (but in that country, the "prior check" can be carried out by an in-house official, if there is one). In these countries, the use of sensitive data combined with a national or other general identifier in a data sharing arrangement would thus often warrant double or even treble prior control by the data protection authority.

The DPA98 too contains a provision which requires some processing operations to be subject to a so-called "preliminary assessment". In the DPA98, the power to decide which processing should be subject to such an assessment has been delegated to the Secretary of State. The latter can issue an order describing certain processing operations that "appear[] to him to be particularly likely – (a) to cause substantial damage or substantial distress to data subjects, or (b) otherwise significantly to prejudice the rights and freedoms of data subjects" (Section 22(1) DPA98).

However, again no such order has been issued. Justice (the UK Section of the International Commission of Jurists) has called for data matching and data processing involving closed-circuit television (CCTV) cameras (and in particular any combination of the two using facial recognition software) to be designated as "assessable processing" (as it is called in the Act).[288] The previous Information Commissioner was of the opinion that "no 'assessable processing' should be designated", i.e. that no processing operations should be made subject to a prior assessment at all.[289] However, the new Commissioner may want to review this position in the light of our findings and of the practice in other countries, briefly summarised above.

C.3 Restrictions on the Taking of Fully Automated Decisions

> *Member States shall grant the right to every person 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, such as his performance at work, creditworthiness, reliability, conduct, etc. (Article 15(1) of the Framework Directive)*

[288] *Justice Briefing* for the second reading of the Data Protection Bill in the House of Lords, February 1998, sections 2.11–2.14.
[289] Summary of the Commissioner's response to the UK Government's *Post-Implementation Appraisal* of the Act, Part B, under the heading *Implementation [of the Directive] in the UK.*

As already noted in Section B, the above provision in the Framework Directive was inspired by French law. Specifically, in France, automated processing of data which involves an assessment of social problems of individuals is subject to "prior authorisation" by the CNIL, and therefore strictly controlled (even if the processing is carried out in the private sector). As we have seen, the CNIL takes a strict view of processing involving an evaluation of young children in particular. The same requirement of "prior authorisation" applies to "automated processing operations which are by their nature, by their scope, or by their purposes, susceptible of depriving persons of a legal benefit ..." – this would apply, for instance, to processing that could lead to the exclusion of a child from school, or to the withdrawal of a social security benefit from a family. In France, the rule in the Directive is thus given real effect, to actual processing operations relating to children. Thus, as we have seen, the "GAMIN" system described in section B, above, had to be abandoned because of the ruling of the CNIL that it breached these data protection principles.

Elsewhere, the rule in the Directive has had more limited application. In Greece and Germany, the decisions covered require a "prior check" – but it is not clear how often such a check is in fact asked for or carried out in these countries (in Germany, the check can in any case be done by an in-house official, if there is one). There are no reports of the provision having been applied in practice, either there or in the other EU Member States that have implemented the Framework Directive, although all the laws include provisions on the lines of Article 15 of the Directive.[290] This would appear to be mainly because of doubts about the scope of the provision: it is clear that it applies only to a narrow range of decisions, i.e. to those in which computers make value-judgmental appraisals of individuals, and not to straight-forward decisions on the basis of objective facts (such as an ATM declining to dispense money because of insufficient funds in the account).

That does not mean, however, that the provision has no bearing on the matters addressed in this study. On the contrary, the unusual data processing and sharing arrangements described earlier could be said to fall within the scope of the rule in the Directive. This is further discussed in section E, with reference to the UK provision implementing Article 15 of the Directive.

C.4 Comparison with the UK

As we have seen, the EC Framework Directive on data protection requires Member States to regulate the use of national identity numbers and other "general identifiers", and many States do impose specific restrictions in this respect. However, although such restrictions can also be imposed under the DPA98 (by means of an order to be issued by the Secretary of State), this has not yet been done. This omission breaches the Directive – which the Information Commissioner might care to point out.

[290] The scope of Article 15 of the Directive is discussed in more detail in D Korff, Data Protection Laws in the European Union, pp. 48–54. For a discussion of the way in which the requirement is phrased in the different laws of the E15 States, see D Korff, Comparative Summary, section 9.4.

Similarly, we have seen that several countries regard the linking or "interconnecting" of databases – and the data sharing this allows – as *ipso facto* posing a risk to the rights and freedoms of individuals, and as therefore requiring a permit or "prior authorisation", or a "prior check" of the processing in question, before such interconnections can be put in place. The DPA98 envisages the imposition of such a measure – to which it refers as a "preliminary assessment" (s. 22) – but again, this has not been done. In this case, the absence of regulation is not, as such, a breach of the Directive, since the Directive only requires States to regulate processing which the States themselves identify as "risky" in this sense. However, the Information Commissioner could take the view that the Secretary of State should use his powers to subject, if not all then at least some, links between public-sector databases to such a "preliminary assessment". This would allow for much stricter regulation and supervision of the databases and data sharing arrangements described in this study, while remaining fully within the framework of the Act.

Can Generating an "Alert" on a Child Fall Within s.12 of the DPA98?

Under the DPA98, the taking of fully automated decisions that have a significant effect on data subjects can be made subject to "preliminary assessment". It is worth examining whether this would have a bearing on the databases and data sharing arrangements discussed in this report.

The DPA98 contains a complex provision, section 12, on the taking of fully-automated decisions. Effectively implementing Article 15 of the Directive, it includes the following rule:

> *Where a decision which significantly affects an individual is based solely on processing by automatic means of that person's personal data for the purpose of evaluating matters relating to him such as, for example, his performance at work, his creditworthiness, his reliability or his conduct, the data controller must as soon as reasonably practicable notify the individual that the decision was taken on that basis, and the individual is entitled, within twenty-one days of receiving that notification from the data controller, by notice in writing to require the data controller to reconsider the decision or to take a new decision otherwise than on that basis.* [291]

To the best of our knowledge, the Information Commissioner has never ruled whether a particular processing operation fell within the scope of this provision. The question arises whether some of the processing described in this report falls within it. This applies in particular to systems that automatically generate an "alert" about a child. This requires that four questions be answered:

[291] Section 12, sub-section (2)(a) and (b), read together with sub-section (1), with the wording slightly simplified by saying "that person's personal data" where the Act says "personal data in respect of which that individual is the data subject".

1. does the raising of an "alert" automatically result in a "decision"?

2. if so, is the decision "based solely on automated processing" of the data on the person(s) (the child or the family) concerned?

3. if so, did the processing involve "evaluating" that person/those persons? and

4. if so, does the decision "significantly affect" the person(s) concerned?

We believe that if certain services or institutions (social services, police) take action on the basis of a certain input, that means that they decided to take action, i.e. that there was a "decision". If the raising of an "alert" in practice automatically results in such action, it can be said that the "alert" caused the action. If the "alert" is generated purely by the application of some kind of algorithm to data entered onto a database (e.g., x number of entries that a professional has information on a child), then it follows that the decision was effectively taken solely on the basis of the automated processing.

The systems we describe furthermore use subjective data on the persons' "conduct", "reliability", etc., and applying an algorithm to such data in our view amounts to an "evaluation" of those matters.

However, one still has to consider what constitutes "action" in this sense, and when a person (child, parent) can be said to be "significantly affected". Taking a child into care of course is obviously action, and obviously significantly affects the child and the rest of the family. We feel that even a visit from a child social worker is action. But is the mere entering of a child on the child protection register action? And do such matters "significantly affect" the child and family? In our view, the answer is yes. This is clear, for instance, from the recently-reported case of a child taken away from a perfectly good mother after being placed on the register and then being taken to hospital.[292] In a ruling several decades ago, the European Commission of Human Rights held that the fact that the police held data on an applicant but had never used or disclosed the data meant that there had not been any interference with the applicant's private life. However, as discussed in Chapter 7, the European Court of Human Rights has clearly revised this position in more recent cases, in which it held that the mere holding of sensitive data on a person constitutes a "serious" interference with that right. We believe that if something constitutes a serious interference with a person's right to private life, it would be odd to hold that that something did not constitute action, or that the decision to take that action didn't constitute a decision, and/or didn't significantly affect the person. In our view, even if an "alert" results only in a file being opened, or a child being placed on a register, that constitutes a "decision" in the sense of s. 12 DPA.

We therefore suggestthat the Information Commissioner too should consider whether the generating of "alerts" *ipso facto* involves the taking of a decision in the sense of Section 12 DPA98. We recommend that the notification form he now uses should be amended to

[292] 'Council must pay £500,000 for wrongly taking girl into care' (see above)

require data controllers to notify him of any processing which falls within the scope of s. 12 – and that he issue guidance on that matter, which makes clear that some of the systems we report fall within the scope of this section. In addition, he should recommend that the Secretary of State designates the taking of decisions of the kind described in s. 12 as "assessable processing" in the sense of s. 22 of the Act, i.e. as the kind of processing that is only allowed after the Information Commissioner has been able to assess it for its compatibility with the Act.

(D) Overall Conclusions

We believe that the law and practice in other countries, described above, can help the Information Commissioner to formulate and support his own position on the matters discussed in this report. In particular, there appears to be widespread agreement between the data protection authorities on the Continent on the following matters:

- Data protection laws and principles should be applied with extra force to data on minors: children deserve extra protection – not less – both because they are more vulnerable and because they are still only "full human beings in the making". It is particularly important to avoid stigmatising children by computer.

- Special care should be taken in seeking consent from minors. The validity of such consent depends on the context, the importance of the matter consented to, and the capacity of the individual child. Involving parents in decisions on under-age children (except in special circumstances) is to be encouraged; failing to involve parents may render the "consent" of a minor invalid and/or the processing "unfair".

- Confidentiality is crucially important in the provision of services to minors and families and professional duties of confidence should therefore not be easily overridden – but if there is a clear risk of actual harm to a child (in the professional judgement of the official or professional considering a disclosure), data can of course be disclosed to counter this. The data protection laws do not stand in the way of such disclosures anywhere.

- By contrast, disclosures and sharing of data on minors for less urgent reasons (such as for social welfare in a broad sense, or for general rather than specific crime prevention) should be strictly limited – and require clear and specific legal authority, preferably in primary legislation. If given under subsidiary legislation, this too should meet the European requirements of clarity, precision, foreseeability and proportionality.

- Such rules should still always allow for the exercise of professional discretion: the law should not seek to take away from the professional his or her proper job to decide what is in the best interest of a child.

- Automated systems tend to do precisely that, even if initially supposedly limited to the generating of indicative "alerts" only. Reliance on automatically generated indicators and "profiles" in the taking of important decisions on children violates their human dignity, identity and personality.

- The use of general identifiers (such as national pupil numbers) facilitates automated data sharing and should therefore be strictly regulated.

- Formal linking of databases *ipso facto* poses risks to the rights and freedoms of the data subjects concerned and should therefore be subject to a "prior check" by the data protection authority.

- The same applies to the taking of fully automated decisions that have a "significant effect" on the data subjects.

We believe that the Information Commissioner might usefully follow his European colleagues in these respects and:

1. confirm the importance of strict data protection for children;

2. clarify the requirements for valid consent by minors, and the need to involve parents whenever possible;

3. stress that disclosures and sharing of data on minors can only be based on specific, clear statutory provisions that reflect the principle of proportionality and respect professional competence and discretion;

4. urge the Government to issue an order under para. 4 of Part II of Schedule 1 to the DPA98, limiting the use of the general identifiers noted in this report, and ask to be consulted on the text of this regulation [NB: the absence of this order is in breach of the EC Framework Directive on data protection];

5. urge the Government to make the linking of (certain) databases subject to a "preliminary assessment" by himself under section 22 of the DPA98; and similarly urge that the taking of fully automated decisions of the kind described in s. 12 DPA98 be made subject to such a "preliminary assessment", with guidance (to be drafted by himself) on the scope of section 12.

These conclusions have informed our analysis of regulatory action options in section 8 above.