Personal Data Protection

Coordinator LDH Ligue des droits de l'Homme

Partners AEDH – EDRI – IURE - PANGEA

United Kingdom national report
EDRi

Bogdan Manolea and Meryem Marzouki

European Digital Rights

December 2009

This publication has been produced with the financial support of the Fundamental Rights &Citizenship program of the European Commission. The contents of this publication are the sole responsibility of LDH, EDRi, AEDH, Pangea, IuRe and can in no way be taken to reflect the views of the European Commission.

I. General Synthesis

I.1. Legislation and Regulations Regarding Privacy

The United Kingdom does not have a written Constitution, but the Human Rights Act 1998[1] provides for incorporation of rights enshrined in the European Convention on Human Rights, including its Article 8 on the right to privacy. This incorporation might however be subject to some derogations and reservations.

Data Protection is ruled by the Data Protection Act 1998[2], as a transposition to the European Data Protection Directive[3]. It applies to both public and private entities. It states eight data protection principles, imposing that anyone who processes personal data must ensure that these data are: fairly and lawfully processed; processed for limited purposes; adequate, relevant and not excessive; accurate and up to date; not kept for longer than is necessary; processed in line with personal rights; secure; and not transferred to other countries without adequate protection. The Act also provides for individual rights with regards to the processing of their personal data, including the right to access these data.

However, these rights have limits in practice. One example has been pointed out by two of our interviewees, Terri Dowty[4] from Actions for the Rights of the Child and David Evans[5], representative of the Information Commissioner Office: children over 12 may file themselves complaints to data controller and exercise their right to access their personal information by filing a "subject access request". This might seem a real advance for the rights, the autonomy and privacy of children and youngsters vis a vis their parents. However, this almost disqualifies complaints and requests when filed by the parents, since the children can file them by themselves. Similarly, when consent is necessary, children over 12 can provide their consent. The question of whether this consent is free and informed is obviously raised here.

The Data Protection Act is considered to be complex, difficult to understand and to use, and not a very effective implementation of the EU Data protection Directive. The UK Information Commissioner's Office has developed a set of FAQs and other documents for the practical application of this Act[6]

The right to privacy and personal data protection in relation with government and public agencies personal information processing is however limited by other pieces of specific legislation. Section 12 of the Children Act 2004[7] on information databases allows for the setting up of national children databases by the government. Other pieces of legislation restricting privacy and data protection rights are referred to in the provided fact sheets of this chapter.

---

[1] Available at <http://www.opsi.gov.uk/acts/acts1998/ukpga_19980042_en_1>.

[2] Available at <http://www.opsi.gov.uk/ACTS/acts1998/ukpga_19980029_en_1>.

[3] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Available at <http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm>.

[4] Interview with Terri Dowty, Director, Action for the Rights of the Child, London, 10/06/09

[5] Interview with David Evans, Senior Data Protection Practice Manager, UK Information Commissioner's Office ICO, London, 11/06/09

[6] Available at <http://www.ico.gov.uk/tools_and_resources/document_library/data_protection.aspx>.

[7] Available at: < http://www.opsi.gov.uk/acts/acts2004/ukpga_20040031_en_1>.

Comprehensive annual reports on privacy in the United Kingdom are published as chapters of the *Privacy and Human Rights* annual reports edited by The Electronic Privacy Information Center & Privacy International[8].

The European Court of Human Rights has ruled some landmark cases against United Kingdom on the basis of Article 8 of the European Convention on Human Rights. In 1984, the Malone ruling[9] against police interception of individuals' communications led to the Interception of Communications Act 1985. In 1997, the Halford ruling against police interception of communications made by a policewoman from her office phone resulted in the adoption of the Regulation of Investigations Power Act (RIPA) 2000[10]; a later ruling[11] of 2007 in the Copland case, again against interception of communications by an employer, noted that when the case was introduced in April 2000, the RIPA was not yet into force. Finally, in a judgement[12] of 4 December 2008 in the Marper case, the European Court of Human Rights ruled that the United Kingdom was breaching Article 8 by holding indefinitely biometric and genetic identifiers of persons arrested for a recordable offence but not found guilty after court proceedings. This ruling has forced the United Kingdom to undertake a process for changing the law accordingly.

I.2. Privacy and Data Protection Control Authorities

The UK Information Commissioner's Office (ICO)[13] is the UK Independent Data Protection Authority as defined in the EU Data Protection Directive. As indicated by the ICO representative when interviewed[14], it is a small organization, although its size has recently doubled. It has less powers than some of its other EU countries counterparts: for instance, although new legislation is in project, the government has currently no obligation to ask for ICO authorization or even opinion before setting up a new database.

The ICO covers four main areas, in relation with the following legislation and regulations: Data Protection Act, Privacy and Electronic Communications Regulations, Freedom of Information Act, Environmental Information Regulations. It publishes annual activity reports[15].

It does not cover important aspects related to privacy and data protection issues, including on the Internet, which fall under the scope of other control authorities, which are: the Chief Surveillance Commissioner (oversight of covert surveillance and human intelligence), the Interception of Communications Commissioner (oversight of interceptions and acquisition of communications data), the Intelligence Services Commissioner, the National Identity Scheme Commissioner (oversight of ID cards and other elements of the National Identity Scheme). In addition, more specialized Authorities exist, such as the Children Ombudsman.

This repartition of roles among different authorities might be a concern in terms of public awareness of issues and risks, and with regards to the transparency and easy access to information. For instance, the oversight of the acquisition of communications data from telecom operators and Internet service providers under the data retention framework is covered by the Interception of Communications Commissioner and not by the ICO. Similarly, issues with the

---

[8] Electronic versions of these reports are available at : <http://tinyurl.com/4zcnd>. Paper versions listed at : <http://epic.org/bookstore/epic_books.html>

[9] Malone v. United Kingdom (1984) 7 EHRR 14

[10] Halford v. United Kingdom (1997) 24 EHRR 523

[11] Copland v. United Kingdom (2007) 45 EHRR 37

[12] S. and Marper v. United Kingdom (2008) ECHR 1581

[13] ICO website available at : <http://www.ico.gov.uk/>

[14] See note 5 above

[15] Available at <http://www.ico.gov.uk/about_us/what_we_do/corporate_information/annual_reports.aspx>

National Identity Scheme are not within the ICO competence, but rather that of the specially appointed Commissioner.
The ICO has developed and made available on its website a range of guidance documents and toolkits, and is spending efforts on raising awareness. However, according to a 2008 survey of the Eurobarometer[16], 80% of UK citizens had not heard of an independent authority in their country monitoring data protection laws.

I.3. Privacy Awareness, Main NGOs and Campaigns

The United Kingdom appears as a paradox. While the "Surveillance Society" is largely documented and opposed, by academics, NGOs, the press, the political opposition, Parliamentary groups and other public and private constituencies, the country shows an "*endemic*" level of surveillance, as rated by Privacy International in a 2007 ranking of 37 countries[17].
The Information Commissioner has confirmed in its 2009 report[18] his 2006 warning that the country was "sleepwalking into as surveillance society". A recent Parliamentary report[19] confirms this danger. A comprehensive study[20] of 46 government databases published in 2009 has found that "*a quarter of the public-sector databases reviewed are almost certainly illegal under human rights or data protection law*" and that "*fewer than 15%*" were "*effective, proportionate and necessary, with a proper legal basis for any privacy intrusions*".
The United Kingdom has a lively civil society with active privacy organizations, such as Privacy International, the Foundation for Information Policy Research, the Open Rights Group, and other well known organizations dealing with privacy as part of their activities, such as Genewatch, Action for The Rights of the Child, Liberty, Statewatch and others. They often join forces to run common campaigns, such as the NO2ID campaign against the National Identity Register and the biometric ID cards. Yet, surveillance and control of the population is increasing, making the United Kingdom a world leader in the adoption of intrusive technologies (biometrics, CCTV, DNA, ...), and in the establishment of nation wide databases, apparently with consent from the population.
The House of Lords report on 'Surveillance: Citizens and the State'[21] provides for a set of recommendations to overcome this situation. Among them, one is directly related to raising privacy awareness: "*We recommend that the Government and local authorities should help citizens to understand the privacy and other implications for themselves and for society that may result from the use of surveillance and data processing. Government should involve schools, learned and other societies, and voluntary organisations in public discussion of the risks and benefits of surveillance and data processing*". Specific awareness actions targeting children and youngsters are particularly needed.

---

[16] European Commission Eurobarometer. Report on Citizen's perceptions on data protection in the European Union, February 2008. Available at: <http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf>
[17] Privacy International, Leading surveillance societies in the EU and the World, December 2007. Available at: <http://tinyurl.com/3bt4a4>
[18] See note 9 above.
[19] House of Lords, 'Surveillance: Citizens and the State', February 2009. Available at: <http://www.publications.parliament.uk/pa/ld200809/ldselect/ldconst/18/18.pdf>
[20] FIPR, 'The database State', March 2009. Availaable at: <http://www.jrrt.org.uk/uploads/Database%20State%20-%20Executive%20Summary.pdf>
[21] See note 13 above, section on 'The role of citizens'.

I.4. Methodology and Presentation of Provided Fact Sheets

As a starting point used to determine the most relevant cases to highlight main trends and most important cases in the United Kingdom, we have used for this study the following sources: articles on UK published in EDRI biweekly newsletter, EDRI-gram[22], information on main UK NGO campaigns, news from UK EDRI members and observers.

After having decided the cases to highlight by providing detailed fact sheets on them, taking into account the project common grid analysis common, we identified some people to conduct in depth interviews with them. These interviews were made in London, on 10-11 June 2009, with: Ms. Terri Dowty, Director, Action for the Rights of the Child (ARCH); Mr. David Evans, Senior Data Protection Practice Manager, UK Information Commissioner's Office (ICO); Mr. Jim Killock, Director, The Open Rights Group (ORG); and Ms. Helen Wallace, Director, Genewatch.

These interviews were complemented with specific researches using the following sources: official documents, Parliamentary debates, reports, public data, relevant organizations websites, press articles, etc.

A general, not UK specific observation is that although the amount of available information on these topics is high, this information is fragmented and scattered among various sources. This highlights the importance and novelty of the research undertaken in the framework of this project, providing fact sheets on different issues and systems. However, this information would need constant update in the future, as legislation in the field is evolving quickly.

An important methodological note regarding the United Kingdom is that there are differences in legislation and regulation in Scotland and Northern Ireland with respect to England and Wales. Such differences are mentioned when applicable in the provided fact sheets.

On mobility and freedom of movement, both the *Automatic Number Plate Recognition System* and the *E-Borders Programme* are detailed. On biological identity, we studied the *National Identity Scheme* and the *National DNA Database*. On interpersonal communications, *Communications Data Retention* has been described, and, as an additional category related to children and youngster registers, we have studied the *ContactPoint Database*.

The chapter on social networks has been worked out in a different format, taking into account the fact that the UK has no special social network focusing only on this territory. We have thus concentrated for this chapter on social networks *usages, local awareness campaigns and reactions* in the UK.

The result of these choices is by no mean exhaustive. The study is not dealing e.g. with CCTV and geo-localization systems and services, nor it addresses the “Oyster” London Travel Card. Many other fact sheets could be included as a follow-up project.

As for the current study, we have preferred to highlight important trends observed in the United Kingdom, to conform to the project objectives mainly addressing children and young people, to allow for comparative analysis between countries studied in the project as a whole, and finally to underline the mutual influence between EU and national level legislation and regulation.

I.5. Conclusions and Recommendations

While the conducted research and the provided fact sheets are by no mean covering all aspects of privacy threats in the UK and should simply be considered as highlighted examples, they allows to draw some general conclusions.

[22] Available at <http://www.edri.org/edrigram>

First of all, privacy and data protection guarantees are rather poor in the United Kingdom, when compared to other EU countries. This especially applies to government databases. The need for establishing stronger guarantees and to reaffirm data protection principles at the EU level is demonstrated, particularly with regards to the purpose limitation principles and to the use of biometric and genetic data, which should be considered as highly sensitive data. The role of the Data Protection Authority should be reinforced, including vis a vis the government, and its oversight should be extended to all privacy and data protection related matters.

Second, the case studied show a high risk of uncontrolled evolution, particularly regarding the use and misuse of government information by private entities for commercial purposes. There should be better protections against this risk.

Third, children and youngster do not seem to benefit from enough protection in the country with respect to their privacy and the protection of their data. The paradox of giving more autonomy to children over 12 by allowing them to file a complaint or a subject access request, or even to give their consent to the processing of some data (e.g. sensitive data in the ContactPoint Database case) has already been mentioned. This issue requires serious examination and debate. Moreover, regarding youngster and adults, the consent requirement is in many cases a fallacy, when giving ones consent is the condition to obtain an essential service, such as education or social and medical welfare.

Fourth, many databases, especially concerning children and young people, are established with the assent of workers who will be using these tools (carers, social workers, educators, doctors,...), since these tools are obviously facilitating their tasks. It seems that awareness campaigns directed towards these workers and their associations are required, to explain that such intrusive surveillance and control means are highly disproportionate with easy management and daily work objectives.

Fifth, awareness campaigns should be directed at children and young adults themselves, so that they are aware of their own rights and how to exercise them in an informed and free manner. It has to be checked, in particular, whether privacy and data protection rights constitutes part of civic education curricula in the country, and if not, the possibility of introducing them should be examined and discussed.

II. Mobility Fact Sheets

II.1. Automatic Number Plate Recognition

THEME	**Mobility**
Identification of technology	**Automatic Number Plate Recognition**
Technology used/tool (For each teams, a card pro tool)	**digital cameras and software similar to Optical Character Recognition (OCR) software to extract the registration data of vehicles**
Country/ use area	United Kingdom
Frame of use	Police
Population concerned: target and age	Vehicle owners
% of users/of young users	Roadside cameras will read 50m plates covering 10m drivers each day, with data recorded for up to five years and a capacity of 18bn licence plate sightings in 2009
Trends (measured / supposed)	Camera based enforcement of speed restrictions increased from just over 300,000 in 1996 to over 2 million in 2004 and raising an estimated £113 million in fines per annum
Known or potentials dangers /Risks	Used to target peace demonstrators ; The system may well lead to a person's vehicle being wrongly identified as associated with known criminals.; Could be use also by private companies in the future. ; Data mining
others	
Generated data bases	
Associated data base/ creation (a line pro database)	The National ANPR Infrastructure includes the following: Back Office Facility (BOF II) which is installed in each police force+ National ANPR Data Centre (NADC) which will receive all the data from force BOFs
What justifies the inscription in the file /Risks?	n/a
Purposes /contents, main data included / Risks?	Scope: to target criminals through their use of the roads, evidence in trials ; seizure of untaxed and unlicensed vehicles, and making a national vehicle movements database part of the National Intelligence Model
File masters? Risks?	Data mining is presently used; PA Consulting (2004) op cit. n.51, suggest that the accuracy read is around 96%, which may sound high, however, even if only one percent of licence plates are incorrectly read and recorded on the data base, this would mean potentially up to half a million erroneous number plates logged each day.
Who accesses the	Every police force in England, Wales, Scotland and Northern Ireland,

files/ Sharing of the data base? Access limits? /Risks	including the British Transport Police. Other Government Department/ Agencies (HMIC, SCDCA, MOD, SPSA, HMRC, SOCA, HMRC and SOCA)
Data retention delays/ risks Right to be forgotten	Data retained for 5 years. The normal period for CCTV is 30 days. The security services have access to all the stored and real time data, they are exempt from the Data Protection Act to use ANPR information
Rights to know or to modify data?	According with Data Protection Act
Covert purposes/ Risks/uncontrolled future evolution	proposal to introduce electronic vehicle identification by means of chips in number plates.
Others (interconnections…)	It has been envisaged its data sharing with the private sector
Legislation in application	
Law /rules / others (?) (implemented for this data base or this technology)	Data protection Act; Association of Chief Police Officers guidelines on the police use of ANPR
Risks for freedoms despite the law	
If revision of the regulation: reasons? Result: improvement or aggravation (compared to the protection of the DP)	The system might be extended for the 2010 Olympic Games
Conformity with the European right (Charter of fundamental rights, directives…)	Not clear
Implementation (or not) of the legislation? / Risks	Yes
Others	
This tools and young public or young adults	
How far are young people concerned?	Not specifically
Awareness of issues or of risks	Information about the existence of CCTV
Indifference or	Mostly indifference ; The primary concern of Civil Liberties groups is

reaction	that the movements of millions of law-abiding people will be recorded and stored on the database for years, a concern that is acknowledged in the "E.C.H.R., Data Protection & RIPA Guidance Relating to the Police use of A.N.P.R." document produced by the ACPO National ANPR User Group.
Awareness campaigns/ results	No evidence that the resulting privacy intrusion brings real crime-reduction gains. Noted with Amber in the Database Report
Good practises	Reducing deaths and injuries on the road
Campaign to be led. On which themes?	Open Rights Group and Privacy International had public positions against the system
Others	
Conclusions	
Recommendations	
References	- 'The Database State' Report, FIPR, March 2009 http://www.jrrt.org.uk/uploads/Database%20State.pdf - NPIA web page on Automatic Number Plate recognition http://www.npia.police.uk/en/10505.htm - SchNEWS, 'Watching You... In Big Brother Britain, 20/03/08 http://www.schnews.org.uk/archive/news6252.htm - 'A Report on the Surveillance Society', Surveillance Studies Network, September 2006 http://news.bbc.co.uk/2/shared/bsp/hi/pdfs/02_11_06_surveillance.pdf - The Guardian, 'Fears over privacy as police expand surveillance project', 15/09/08 http://www.guardian.co.uk/uk/2008/sep/15/civilliberties.police - BBC News, 'Camera grid to log number plates', 22/05/09 http://news.bbc.co.uk/2/hi/programmes/whos_watching_you/8064333.stm - ACPO National ANPR User Group, 'E.C.H.R., Data Protection & RIPA Guidance Relating to the Police use of A.N.P.R., October 2004 http://www.steve-kane.co.uk/words/misc/ANPR-Oct-2004.pdf Open Rights Group web page on Nationa Vehicle Tracking Database : http://www.openrightsgroup.org/orgwiki/index.php/ National_Vehicle_Tracking_Database

II.2. Travel Record Database/PNR- E-Borders Program

THEME	**Mobility**
Identification of technology	**Travel Record Database**
Technology used/tool (For each teams, a card pro tool)	**E-Borders Program**
Country/ use area	UK
Frame of use	UK Border Agency (Home Office Border and Immigration, in cooperation with HR Revenue and Customs and the Police). The E-Borders programme intends to electronically collect and analyse information from carriers (including airlines, ferries and rail companies) about passengers who intend to travel to or from the UK before they travel. These data are checked against watch list. It can be seen as a UK PNR programme. The programme will be progressively implemented from 2008 to 2014. Data is collected from carriers on passengers, crews and freight.
Population concerned: target and age	Everyone who intends to travel to/from the UK by air, see or rail. The Common Travel Area (CTA, ruled by an agreement between the UK, Ireland, the Isle of Man and the Channel Islands, allowing passport-free movement), remains however free from immigration controls on people travelling from within the area. The UK government tried to introduce passport control in the CTA in the Borders, Citizenship and Immigration Bill, but this clause was rejected by Parliament. The government expressed however its intentions to bring back the issue to the Parliament, after the Borders, Citizenship and Immigration Act was adopted in July 2009.
% of users/of young users	No data yet. Since every traveller is concerned, the % of young users will be the one of the % of young users travelling.
Trends (measured / supposed)	No data yet, but this programme will concern every traveller, which means potentially everyone in the world. This kind of programme is part of the overall UK system of people's movement surveillance, in addition to the IRIS automated entry system and the biometric passports scheme. At the international level, there is an increasing trend for people's movement control (US-EU PNR, other countries, such as Spain and France PNR schemes, EU PNR scheme, international standards for biometric passports, biometric visa system,..)
Known or potentials dangers /Risks	Same dangers as those identified in the US-EU PNR system, including: risk of illegitimate search of passengers, risk of illegitimate prevention of travelling, ethnic and other sensitive information-based profiling, interconnection with other databases, use of the information for illegitimate purposes,..

	Same risks as for other UK database (security of data is poor, leading to losses of huge amount of people's data). Specific dangers and risks: the e-borders programme is not only targeting foreign travellers, but also UK citizens and residents, and is operated in cooperation with the police and the revenues and customs office. Consequently, in addition to immigration and border control, it aims at internal police and at internal revenues and customs control objectives. There is a risk that the system and date sharing be extended to other governments agencies, such as those in charge of work and pensions, or health, in order to track people claiming benefits in the UK while leaving abroad or seeking NHS treatment they are not entitled to. Furthermore, these objectives include prevention purposes, not necessarily of crimes but also of simple disorders, which might lead to totally illegitimate and disproportionate control of UK citizens and residents, simply because of their travel profile. Moreover, in addition to passenger's data, the programme will collect and analyse freight data. This would allow for the control of shipped goods, and for the identification of the parties involved in any kind of such transaction, which might lead to reveal sensitive details (e.g. related to health or sexual-life). In general, the system will allow to conduct intelligence tasks based on the travel history and movements of people, which could be used as evidence for judicial proceedings.
others	
Generated data bases	
Associated data base/ creation (a line pro database)	E-Borders Operations Centre (E-BOC) database
What justifies the inscription in the file /Risks?	Travelling and shipping to or from a UK border, by air, see or rail. For risks, see above.
Purposes /contents, main data included / Risks?	Purposes: fight against irregular immigration, visa processing, policing purposes, customs. Purposes. Purposes are detailed below by Agency. Contents: detailed information on people's travel document, detailed data on the reservation made, information on the travel means (flight, train or ship), information on vehicle carried on a voyage (e.g. by ferry or train), travel history, and information related to freight (including the parties in the transaction). These categories of data are detailed below. They include sensitive data. Risks: the amount of collected data, including for intelligence purposes, is in itself a high factor of risk. There is first a risk for the security of these data, and experience has shown that they

	are not sufficiently protected in the UK (25 million child benefit records were lost by Revenues and Customs in 2007). Second, these data contains or can easily reveal sensitive information as identified in the UK Data Protection Act (commission or alleged commission of offences, religious belief, health, ethnicity, sexual life). Third, the data contains banking details. Fourth, they contain entire travel history of a person, which could be used as a criteria for tougher controls or even travel prevention. Fifth, they contain information of people in contact with the traveller (either because they travel together, or because they made the reservation, or even when they are the guardians of a minor travelling alone). Furthermore, the e-borders programme purposes are wide enough to allow every possible use of the collected data, far beyond the claimed objectives. Detailed information below are provided in the Code of practice, see references. Detailed purposes by Agency: Border and Immigration Agency: Criminal investigations on groups and individuals involved in abuse of the immigration system and linked to criminality; Analysis of patterns and trends to help detect activity worthy of further investigation or intervention; Passenger audit and compliance, where data is used as intelligence to identify those who overstay or claim asylum some years after they have arrived. It is also used to confirm a person's previous compliance with conditions of entry and, therefore, inform future risk assessments. UKVisas: Ready access to historical data to expedite processing of such visa applications and directly inform the decisions made by Entry Clearance Officers. Police: 'Policing purposes', which means: (i) The prevention, detection, investigation or prosecution of criminal offences; (ii) Safeguarding national security; (iii) Such other purposes as may be specified by order of the Secretary of State. In practice the police will use the information for enquiries in connection with: the prevention and detection of serious crime; the protection of vulnerable victims and witnesses; and the execution of warrants and enforcement of other judicial orders. The information will also be used to: identify travellers for intelligence and intervention purposes; support intelligence and operational activity; and inform on matters regarding the border and

	deployment of police resources. Revenues and Customs: (i) The prevention, detection, investigation or prosecution of criminal offences; (ii) The prevention, detection or investigation of conduct in respect of which penalties which are not criminal penalties are provided for by or under any enactment; (iii) The assessment or determination of penalties which are not criminal penalties; (iv) Checking the accuracy of information relating to, or provided for purposes connected with, any matter under the care and management of the Commissioners or any assigned matter; (v) Amending or supplementing any such information (where appropriate); (vi) Legal or other proceedings relating to anything mentioned in paragraphs (i) to (v); (vii) Safeguarding national security; and (viii) Such other purposes as may be specified by order of the Secretary of State. Information shared with HMRC under the IAN provisions will be used to: identify individuals or companies involved in the smuggling of, amongst others, Class A drugs, criminal cash, and prohibited or restricted goods such as firearms, offensive weapons, paedophile material and products of animal origin; and target smuggling of cigarettes, hand rolling tobacco, alcohol, oils and high-risk counterfeit goods. HMRC's other statutory functions at the border such as the detection of VAT missing trader fraud and the operation of screening equipment to detect illicit movements of nuclear or radiological material will all be supported by access to data shared. Detailed content: Data categories (collected from carriers): 1/ Information about a passenger's or crew member's travel document or journey a) Travel Document Information (TDI). Carriers will be required to collect and transmit all TDI data to the border agencies. TDI refers to a passenger's or crew member's biographic and travel document details, normally contained in the machine-readable zone of a passport or other travel document (details of which are set out below). □ Full name □ Gender

	□ Date of birth □ Nationality □ Type of travel document □ Travel document number □ Travel document issuing state □ Travel document expiry date Where the passenger or a member of crew does not hold a travel document, information must be provided regarding the type of identification relied upon together with the number, expiry date and issuing State of that identification. b) Other Passenger Information (OPI). Provided by the carrier to the extent that it is known to them. □ name as it appears on the reservation; □ place of birth; □ issue date of travel document; □ address; □ sex; □ any contact telephone number; □ e-mail address; □ travel status of passenger, which indicates whether reservation is confirmed or provisional and whether the passenger has checked in; □ the number of pieces and description of any baggage carried; □ any documentation provided to the passenger in respect of his baggage; □ date of intended travel; □ ticket number; □ date and place of ticket issue; □ seat number allocated; □ seat number requested; □ check-in time, regardless of method; □ date on which reservation was made; □ identity of any person who made the reservation; □ any travel agent used; □ any other name that appears on the passenger's reservation; □ number of passengers on the same reservation; □ complete travel itinerary for passengers on the same reservation; □ the fact that a reservation in respect of more than one passenger has been divided due to a change in itinerary for one or more but not all of the passengers;

	□ Code Share Details; □ method of payment used to purchase ticket or make a reservation; □ details of the method of payment used, including the number of any credit, debit or other card used; □ billing address; □ booking reference number, Passenger Name Record Locator or other data locator used by the carrier to locate the passenger within its information system; □ the class of transport reserved; □ the fact that the reservation is in respect of a one-way journey; □ all historical changes to the reservation; □ General Remarks; □ Other Service Information (OSI); □ System Service Information (SSI) and System Service Request information (SSR); □ identity of the individual who checked the passenger in for the voyage or flight or international service; □ Outbound Indicator, which identifies where a passenger is to travel on to from the United Kingdom; □ Inbound Connection Indicator, which identifies where a passenger started his journey before he travels onto the United Kingdom; □ the fact that the passenger is travelling as part of a group; □ the expiry date of any entry clearance held in respect of the United Kingdom; □ card number and type of any frequent flyer or similar scheme used; □ Automated Ticket Fare Quote (ATFQ), which indicates the fare quoted and charged; □ the fact that the passenger is under the age of eighteen and unaccompanied; and □ where the passenger is a person under the age of eighteen and unaccompanied— □ age; □ languages spoken; □ any special instructions provided; □ the name of any departure agent who will receive instructions regarding the care of the passenger; □ the name of any transit agent who will receive

	instructions regarding the care of the passenger; □ the name of any arrival agent who will receive instructions regarding the care of the passenger; □ the following details in respect of the guardian on departure— □ name; □ address; □ any contact telephone number; and □ relationship to passenger; and □ the following details in respect of the guardian on arrival— □ name; □ address; □ any contact telephone number; and □ relationship to passenger. c) Service Information (SI) Service information is information related to the flight, train or ship the passenger or crew member is travelling on. This information must be provided by the carriers in all cases for both inbound and outbound journeys: □ Flight number, train service number or ship name or carrier running number □ Name of carrier □ Nationality of ship □ Scheduled departure date and time □ Scheduled arrival date and time □ Place and country from which the flight, journey or voyage departed immediately prior to arrival into the United Kingdom □ Place in the United Kingdom where the flight, journey or voyage first arrives from overseas □ Any place in the United Kingdom where a flight, journey or voyage which has arrived into the United Kingdom from overseas will subsequently go □ Number of passengers. d) Additional information regarding passenger's and crew vehicles and members of crew

	Carriers will be required to submit the vehicle registration mark (VRM) in respect of any vehicle in which a passenger or member of crew is travelling and which is carried on a service or voyage, together with the registration number of any trailer attached to that vehicle. Carriers will also be required to inform the Border and Immigration Agency of the number of crew on a flights, journey or voyage, the place of birth and rank of a member of crew. 2/ Information held by the border agencies, which relate to a passenger or crew member or their journey or a freight movement This may include information such as historical data from previous journeys/movements or intelligence on suspect individuals/vehicles. 3/ Information about or related to freight This will include details about the freight movement, including the parties involved in the transaction and details about the goods being moved (e.g. description, weight, origin, value, route taken to the UK etc).
File masters? Risks?	E-Borders Operations Centre (E-BOC), which is a common centre of all UK border agencies. It should be noted that the E-Borders system development and most probably maintenance has been contracted to a industry consortium names Trusted Borders, and led by a UK subsidiary of Raytheon Systems Limited, a US company. Raytheon Systems Limited of the UK is a major supplier to the U.K. Ministry of Defence. Furthermore, according to the UK Home Office Border Agency web pages on E-Borders, intentions are clear to "market e-Borders widely internationally" and " address any issues in requesting data from certain countries on an individual basis through established communication channels."
Who accesses the files/ Sharing of the data base? Access limits? /Risks	Data is electronically available to officers of the border agencies who are based within E-BOC. Other border agency staff with "appropriate security clearance within the E-BOC" will routinely allowed to view the data, made enrichments and interpretation to produce alerts for dissemination. The border agencies with which data may be shared are: Border and Immigration Agency, UKVisas, the Police, HM Revenue and Customs.
Data retention delays/ risks Right to be forgotten	E-BOC retains data for 5 years, and data are automatically removed after this period. Earlier deletion might occur upon

	specific audits. However, when data is transferred to another border agency, the retention period is then governed by this agency own rules. The Border an Immigration Agency and UKVisas keep the data for 5 years, with flexibility to allow access for this data for another 5 years on a case by case basis. The Police and the Revenue and Customs require data to be held for "as long as it is relevant", for "policing purposes" and customs purposes, respectively. This means that data might be potentially kept for an infinite period of time, which seriously compromises the right to be forgotten.
Rights to know or to modify data?	Right to know can be exercised by sending a "subject access request" (SAR) to e-BOC, in conformity with the data protection Act. When a subject record has been enriched by another agency, then the addition information could be accesses through a SAR made to the concerned agency. Exceptions to the disclosure of the information provided by the Data Protection Act applies.
Covert purposes/ Risks/uncontrolled future evolution	Use as routine intelligence tool for any kind of purpose, even small infractions. Future evolution will certainly include biometric data, because of biometric passports and biometric ID cards.
Others (interconnections…)	High level of interconnection and data sharing between agencies.
Legislation in application	
Law /rules / others (?) (implemented for this data base or this technology)	There is no specific law regarding the E-Borders programme, established in 2005 by the Home Office. Legal provisions for requesting passenger information from carriers are contained in: the Immigration, Asylum and Nationality Act 2006; the Immigration and Asylum Act 1999; the Immigration (Passenger Information) Order 2000; the Revenue and Customs Commissioners' Directions; Schedule 7 to the Terrorism Act 2000 (Information) Order 2002; Sections 36 and 37 of the Immigration, Asylum and Nationality Act 2006. They are further detailed in the 'Code of practice on the management of information shared by the Border and Immigration Agency, Her Majesty's Revenue and Customs and the police'
Risks for freedoms despite the law	Important risks of interconnection and use by other government services and private companies. Important Risk of extra check and even travel denying of people. Profiling. Breach of freedom of movement principle.
If revision of the regulation: reasons? Result: improvement or aggravation (compared to the protection of the DP)	The UK Border Agency was created in 2008 by the Home Office as a 'Security Global Hub' to integrate the work of the Border and Immigration Agency, Ukvisas, and border related work of HM Revenue and Customs.

	The Borders, Citizenship and Immigration Act 2009, adopted in July 2009, has given custom powers to the UK border agency, and 4500 Revenues and Customs staff will be part of the Agency. This means a true mix of immigration and revenue and customs matters, even beyond usual customs detection work at the boards. Further legislative steps are expected, in the framework of the 'simplification project' in view of reforming the immigration law. In this context, like it happened by the Borders, Citizenship and Immigration Act 2009, further powers could be granted to the UK Border Agency. Finally, biometric data will be included in the scheme as biometric passports and ID cards are being developed.
Conformity with the European right (Charter of fundamental rights, directives…)	The E-Borders programme might infringe the right of free movement enshrined in EU legislation. Since all data should be provided by carriers, this might also infringe some EU countries law providing that only law enforcement officials might gather passport data (this concern has been expressed by the Eurostar company to the UK Parliament, in reference to the French and Belgian law). The Guardian and the Observer reported on 12 July 2009 that a letter from Ernesto Bianchi, acting head of the EC DG Justice, Freedom and Security, "raises doubts about the legality of asking passengers for anything other than their passport", and that the E-borders scheme "risks breaching European law because it restricts the right to free movement".
Implementation (or not) of the legislation? / Risks	N/A
Others	
This tools and young public or young adults	
How far are young people concerned?	Not specifically targeted.
Awareness of issues or of risks	Little awareness.
Indifference or reaction	Mostly indifference. However, newspapers regularly report on the cost and probable inefficiency of the scheme. They also report about the 'travel chaos' that it will create at frontiers, especially during holidays season. Most recently, fears have been expressed that the scheme could, eventually, abolish the control-free travel inside the CTA.
Awareness campaigns/ results	No real awareness campaigns. Privacy International and Statewatch mainly reacted upon first announcement of the program in 2005. 'Our world our say' launched a petition against the program, but there is no information on how many signatures have been collected.

Good practices	None
Campaign to be led. On which themes?	The US-EU PNR agreement has raised great concerns since 2003, while 'national PNR' plans have received relatively less attention. A campaign at the EU level, making the links between the US-EU PNR, the EU plans and national schemes would probably be a good way to raise awareness. Consumer organizations should certainly be included in such campaigns. The main theme of the campaign could be freedom of movement, while the campaign should highlight that sensitive data are collected and analyzed.
Others	
Conclusions	The E-borders scheme is a perfect illustration of the drift of control and surveillance from some specific threats (security, fight against terrorism) to a large number of other purposes of less legitimacy with respect to the surveillance means used.
Recommendations	Better guarantees needed (probably at EU level) for the respect of freedom of movement provisions, especially inside the EU.
Sources	
Références	- UK Border Agency (http://www.ukba.homeoffice.gov.uk) - Code of practice on the management of information shared by the Border and Immigration Agency, Her Majesty's Revenue and Customs and the police (http://www.ukba.homeoffice.gov.uk/sitecontent/documents/managingourborders/eborders/codeofpractice) Statewatch bulletin vol.15, n.3/4, August 2005 (http://www.statewatch.org/news/2005/aug/ebord.pdf) Privacy International Comments, July 2005 (http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-260609). - E-Borders advertising document by the industry consortium selected to develop the technology (http://www.trustedborders.com/documents/exporting-the-border.pdf) - "Lords defeat for e-borders scheme" (http://www.publicservice.co.uk/news_story.asp?id=9086). - 'Our World Our Say' petition (http://www.ourworldoursay.co.uk/e-borders.php) - Eurostar and other carriers oral evidence given to the House of Commons, 30/06/09 (http://www.publications.parliament.uk/pa/cm200809/cmselect/cmhaff/uc817/uc81702.htm). - Guardian and Observer article, 12/07/09 (http://www.guardian.co.uk/uk/2009/jul/12/uk-borders-european-law-eborders)

III. Biological Identity Fact Sheets

III.1. Biometrics – UK National Identity Service

THEME	**Biological identity**
Identification of technology	**Database/Biometrics**
Technology used/tool (For each teams, a card pro tool)	**UK National identity Service**
Country/ use area	UK
Frame of use	National registry, National ID Card, biometric passport, benefit of e-government services, as well as private electronic transactions, such as opening a bank account.
Population concerned: target and age	Whole population, citizens and foreign residents, aged more than 16.
% of users/of young users	According to population.
Trends (measured / supposed)	The implementation scheme is still in development.
Known or potentials dangers /Risks	There are less safeguards against interconnections and information exchanges in the UK than in other countries where constitutional protections exist. The risk is thus high that the unique number contained in the identity register may lead to interconnections of information in public and private sectors databases. Further, the biometric data contained in the Register make these risks higher.
others	
Generated data bases	
Associated data base/ creation (a line pro database)	UK National Identity Register
What justifies the inscription in the file /Risks?	Mandatory registration, for citizens and foreign residents, starting from age 16.
Purposes /contents, main data included / Risks?	Purpose: Identification and authentication of population, by public services as well as by employers and private services. Contents (no sensitive personal data): (a) identity (full name; other names by which the person has previously been known; gender; date and place of birth and, if the person has died, the date of his death; and external characteristics of his that are capable of being used for identifying him.) (b) address of principal place of residence in the United Kingdom;

	(c) address of every other place in the United Kingdom or elsewhere where the person has a place of residence; (d) where in the United Kingdom and elsewhere the person has previously been resident; (e) the times at which the person was resident at different places in the United Kingdom or elsewhere; (f) current residential status (nationality; entitlement to remain in the United Kingdom; and where that entitlement derives from a grant of leave to enter or remain in the United Kingdom, the terms and conditions of that leave.); (g) residential statuses previously held by the person; (h) information about numbers allocated to the person for identification purposes and about the documents to which they relate; (i) information about occasions on which information recorded about the person in the Register has been provided to any person; and (j) information recorded in the Register at the person's request. Biometrics, including facial image and fingerprints, will be recorded, too. Risks: interconnection with other databases, full history of a person is recorded, biometric data. One important risk is that the Identity Card Act 2006 does not provide for any limitation of the amount and kind of biometric identifiers to be collected and recorded. The Act simply provides that: "The things that an individual may be required to do under subsection (X) are [...] (b) to allow his fingerprints, and other biometric information about himself, to be taken and recorded; (c) to allow himself to be photographed; (d) otherwise to provide such information as may be required by the Secretary of State.". This means that these limitations (if any) would be provided by the administration through the concerned government agencies, and not by law.
File masters? Risks?	UK Home Office Identity and Passport Service, although it is not clear yet whether other agencies will hold some of the data. Whether the data are centralised or decentralised, a unique number will allow to create full audit trails of people's interactions with services.
Who accesses the files/ Sharing of the data base? Access limits? /Risks	According to the Identity and Passport Service, government agencies and private businesses will be able to check the information held on the national identity register, in order to help them establish the identity of their customers and staff. For example, when opening a bank account or registering with a doctor. The National Identity Register will then be widely accessed, and this carries a high risk of disclosure and misuse of personal data.
Data retention delays/ risks Right to be forgotten	Data are kept permanently, including after the death of the person. A full history of the person is recorded.
Rights to know or to modify data?	According to the Data protection act.

Covert purposes/ Risks/uncontrolled future evolution	The Register will be used to issue ID cards and Passports. Covert purposes include policing purposes, and fight against irregular immigration and fraudulent use of social benefit. The Act leaves open the possibility to include additional data, including additional biometric identifiers. The fact that employers and private service providers, such as banks, medical insurance companies, etc. may access the Register for identification and authentication purposes opens the way for any uncontrolled evolution or misuse.
Others (interconnections…)	No data yet. The scheme is only starting to be developed.
Legislation in application	
Law /rules / others (?) (implemented for this data base or this technology)	Identity Card Act 2006.
Risks for freedoms despite the law	Important risks of interconnection and use by potentially all public and private services. Record of all interactions of an individual with services. Full transparency of individuals vis a vis public and private services. Presumption of accuracy of the registered data. If fully implemented, the scheme would lead to the denial of any kind of anonymity.
If revision of the regulation: reasons? Result: improvement or aggravation (compared to the protection of the DP)	No revision yet.
Conformity with the European right (Charter of fundamental rights, directives…)	The scheme is rated as 'red' in the 'Database State' report, which means that the concerned database is 'is almost certainly illegal under human rights or data protection law and should be scrapped or substantially redesigned. The collection and sharing of sensitive personal data may be disproportionate, or done without our consent, or without a proper legal basis; or there may be other major privacy or operational problems'.
Implementation (or not) of the legislation? / Risks	Still in early stages. Biometric passports and identity cards for foreign residents are starting to be issued.
Others	
This tools and young public or young adults	
How far are young people concerned?	Everyone over 16 is concerned.
Awareness of issues or of risks	High awareness of risk. A poll conducted in June 2008 indicates only 50% support to the scheme in the population (support was 80% when ID cards, which are part of the scheme, were suggested).

Indifference or reaction	Huge opposition since early proposals of the scheme. The UK has no identity cards since 1952.
Awareness campaigns/ results	Main campaign has been jointly conducted by many civil liberty organizations under the 'NO2ID' UK-wide, non-partisan coalition. Academics (most notably at LSE), Parliamentarians and the Press also played a major role. The result of the awareness is an important decrease of support to the scheme in the population. The opposition has declared in July 2009 at a Parliament session their intention to abolish the scheme if they come into power. The implementation of the scheme seems to be slower than expected, and that portions of the population are threatening industrial action if they are forced to register: this is the case of airport workers and pilots, who are expected to be registered in the next step of the scheme development, after foreign residents.
Good practises	None
Campaign to be led. On which themes?	The ID Cards and national identity registers based on biometrics are being proposed not only in the UK, but also in other EU countries. Although the schemes vary across countries with different history, a campaign against biometric identity is probably needed at the EU level.
Others	
Conclusions	Centralized registers and biometric ID cards
Recommendations	Need for a better guarantees at EU level against such a generalization of the use of biometric identity and centralized registers. The possibility of access to such information by almost all public service agencies, as well as private business is of special concern.
References	- Home Office Identity and Passport Service (http://www.ips.gov.uk) - FIPR, 'The Database State' Report, March 2009 (http://www.jrrt.org.uk/uploads/database-state.pdf) - NO2ID campaign website (http://www.no2id.net) - ICM Poll for No2ID, 25-26/06/08 (http://www.icmresearch.co.uk/pdfs/2008_june_no2id_poll.pdf) - ZDNet Article, 'Tories plan to scrap National Identity Register', 13/07/09 (http://news.zdnet.co.uk/security/0,1000000189,39674798,00.htm)

III.2. DNA - UK Police National DNA Database (NDNAD)

THEME	**Biological identity**
Identification of technology	**DNA**
Technology used/tool (For each teams, a card pro tool)	**UK Police National DNA Database (NDNAD)**
Country/ use area	UK (mainly England and Wales). The database is not fully implemented in Northern Ireland, and significant differences exist in Scotland.

<table>
<tr><td>Frame of use</td><td>UK Police. It collects 2 DNA samples, and send them for analysis to a private, accredited laboratory. The laboratory sends back a non coding DNA profile to the police, and keeps the second sample in a database for "research" purpose. Samples may be taken from an identified individual, or from a crime scene.</td></tr>
<tr><td>Population concerned: target and age</td><td>Anyone more than 10 years old, arrested on suspicion of any recordable offence. DNA samples are taken without consent. In addition, the police can ask people to voluntarily give a sample of their DNA as a way of eliminating them from enquiries, or give an additional signature if they agree to having their DNA profile added to the database. In Scotland volunteers can change their minds and ask to be removed from the Database, but this is not possible in England and Wales.</td></tr>
<tr><td>% of users/of young users</td><td>As of January 2009 in England and Wales (Parliamentary debates): 4.5 million individuals (7% of the total UK population). Gender breakdown: 78.6% Male, 20.7% Female. Cumulative percentage by age: 2.5% under 16, 6.5% under 18, 15.3% under 20, 29.5 under 25 and 60% under 35. Percentage by ethnic appearance: 6.1% Asian, 7.7% Black, 0.8 Middle-Eastern and 79.5 White. These percentages need to be compared to the ethnic appearance in the total population: according to Genewatch, about 30% of the black population aged over 10 had their DNA profile on the database in November 2008. The Guardian reported in 2006 that while 30% of the black men were on the database, only less than 10% of the white men were recorded.</td></tr>
<tr><td>Trends (measured / supposed)</td><td>NDNAD is the largest DNA database of any country and UK had the largest proportion of its population’s DNA held on a database. This proportion increased from 5.4% in 2005 (EU average: 1.1%, USA: 0.5%) to more than 7% in end 2008. Another indication of this trend is the increase of DNA profiles (number of individuals being estimated using a constant 13.3% replication rate): from approximately 2.4 millions in 2003/2004, the number doubled in 5 years, reaching more than 5 millions in 2008/2009.
The following table (figures until May 2007 for England and Wales only, source: Hansard), shows the number of people added to NDNAD yearly.
<table>
<tr><td>Age</td><td>Under 16</td><td>16 to 18</td><td>19 to 20</td><td>21 and over</td><td>Total</td></tr>
<tr><td>1995-96</td><td>2,507</td><td>5,977</td><td>3,923</td><td>21,718</td><td>34,127</td></tr>
<tr><td>1996-97</td><td>4,964</td><td>14,137</td><td>9,511</td><td>52,968</td><td>81,588</td></tr>
<tr><td>1997-198</td><td>7,886</td><td>20,152</td><td>12,888</td><td>85,97</td><td>126,909</td></tr>
<tr><td>1998-99</td><td>18,764</td><td>37,696</td><td>24,395</td><td>152,964</td><td>233,828</td></tr>
<tr><td>1999-2000</td><td>21,055</td><td>31,902</td><td>20,29</td><td>121,761</td><td>195,011</td></tr>
<tr><td>2000-01</td><td>47,735</td><td>59,088</td><td>37,978</td><td>233,312</td><td>378,119</td></tr>
<tr><td>2001-02</td><td>60,972</td><td>70,534</td><td>43,93</td><td>296,445</td><td>471,896</td></tr>
<tr><td>2002-03</td><td>55,226</td><td>62,823</td><td>38,844</td><td>287,468</td><td>444,394</td></tr>
<tr><td>2003-04</td><td>56,033</td><td>59,403</td><td>36,911</td><td>279,35</td><td>431,723</td></tr>
<tr><td>2004-05</td><td>68,381</td><td>66,954</td><td>37,542</td><td>307,393</td><td>480,286</td></tr>
<tr><td>2005-06</td><td>87,459</td><td>86,052</td><td>49,801</td><td>402,427</td><td>625,797</td></tr>
<tr><td>2006-07</td><td>90,919</td><td>88,522</td><td>51,005</td><td>437,229</td><td>667,737</td></tr>
<tr><td>Total as of May 2007</td><td>521,901</td><td>603,24</td><td>367,018</td><td>2679,005</td><td>4171,415</td></tr>
</table></td></tr>
</table>

This second table, where previous table figures have been computed, shows that the number of registered people aged under 16 is growing faster each year than in the other age range.

Year	% increase under 16	% increase 16-18	% increase 19-20	% increase 21 and over	% increase total
1996-97	98	137	142	144	139
1997-98	59	43	36	62	56
1998-99	138	87	89	78	84
1999-2000	12	-15	-17	-20	-17
2000-01	127	85	87	92	94
2001-02	28	19	16	27	25
2002-03	-9	-11	-12	3	-6
2003-04	1	-5	-5	-3	-3
2004-05	22	13	2	10	11
2005-06	28	29	33	31	30
2006-07	4	3	2	9	7

Known or potentials dangers /Risks	Dangers and risks inherent to DNA and other biometric databases: DNA matches between crime scenes and individuals on the Database include matches with victims and passers-by and false matches, so equating matches with criminals is misleading. The sample analysis by commercial laboratories, even though accredited, is also an issue. The 'familial searching' practice, in view of matching DNA samples from a crime scene with one individual relatives when the individual is not on the database, carries the risk of revealing non-paternity cases. In addition, transfer to other countries of profiles to other countries is increasing (inter alia through the introduction of main provisions of Prüm Treaty in EU legislation).
others	
Generated data bases	
Associated data base/ creation (a line pro database)	UK Police National DNA Database (NDNAD)
What justifies the inscription in the file /Risks?	Crime scene or arrest for any recordable offence. This includes begging, being drunk and disorderly and taking part in an illegal demonstration. This means that particular segments of the population are targeted: youngster, poors, activists..
Purposes /contents, main data included / Risks?	DNA samples from crime scenes and non coding DNA profiles of individuals. For individuals, additional information are: name, date of birth, ethnic appearance, ethnic code (White - North European; White - South European; Black; Asian; Chinese, Japanese, or other South East Asian; Arabic or North African; Unknown).
File masters? Risks?	UK National Policing Improvement Agency (NPIA).
Who accesses the	UK National Policing Improvement Agency (NPIA), with general oversight by

files/ Sharing of the data base? Access limits? /Risks	the NDNAD Strategic board (representatives of the Home Office, the Association of Chief Police Officers, the Association of Police Authorities, and the Human Genetics Commission). Operation and maintenance of the NDNAD is the responsibility of the Forensic Scientific Service (FSS). Any police force submitting a DNA sample get a report of any hit matching an individual profile or a sample in the NDNAD.
Data retention delays/ risks Right to be forgotten	Apart from Scotland, DNA is kept permanently, even if the person is eventually not charged or acquitted.
Rights to know or to modify data?	Right to know can be exercised by sending a "subject access request" to the local police station, in conformity with the data protection Act. The UK DPA provides samples to write such letters.
Covert purposes/ Risks/uncontrolled future evolution	Use of the database by the police as a routine intelligence tool, in search for a better ratio of solved crimes and crime prevention strategy. Provoking arrests to store more DNA profiles to this end. Considering any youngster as potential criminal. Ethnic bias. According to Genewatch, there is strong government support on getting everyone's DNA.
Others (interconnections…)	In January 2009, the UK government proposed a draft Bill ('Coroners and Justice Bill), allowing medical records, genetic information and DNA collected in the NHS to be shared with any organisation or individual, including private companies, foreign governments and the police, without people's consent or knowledge. Following controversy, this draft Bill was withdrawn in March 2009.
Legislation in application	
Law /rules / others (?) (implemented for this data base or this technology)	NDNAD established by the Criminal Justice and Public Order Act in 1994. Main amendments by the 1996 Criminal Procedure and Investigations Act, the 1997 Criminal Evidence Act, the 2001 Criminal Justice and Police Act, the 2003 Criminal Justice Act, the 2005 Serious Organised Crime and Police Act and the Counter-Terrorism Act 2008.
Risks for freedoms despite the law	Important risks of interconnection and use by other government services and private companies. According to Genewatch, 23andme US company (funded inter alia by Google) has been in discussion with the UK government.
If revision of the regulation: reasons? Result: improvement or aggravation (compared to the protection of the DP)	Continuous aggravation: In 1997, the revision allowed to take samples without consent from prisoners convicted for a sex, violence or burglary offence before NDNAD set up. In 2001, the revision allowed for permanent retention of profiles, even those of acquitted individuals and those of volunteers having freely given their consent. In 2003, sample taking without consent has been extended to cases of simple suspicion of recordable offences, with permanent retention even without eventual charges. In 2005, the NDNAD could include identification of deceased persons. In 2008, the revision allowed to collect samples from persons subject to control orders, and during any authorised secret surveillance, with permanent retention. It also allowed to search samples against material held by security or intelligence services, and to use them for national security purposes. Required improvement, most notably with regards to retention

	delays and age of recorded individuals: conformity to the ECHR judgement of December 2008.
Conformity with the European right (Charter of fundamental rights, directives…)	The European Court of Human Rights has ruled that it is illegal for the Government to keep all this personal information from innocent people (Marper case, 4 December 2008). The government launched a consultation in May 2009 on its proposal to take into account this judgement in the national law.
Implementation (or not) of the legislation? / Risks	The Uk government is late in taking into account the ECHR judgement in national law, and will probably only partially implement it.
Others	
This tools and young public or young adults	
How far are young people concerned?	60% of the individuals whose DNA profile is recorded are under 35. Number of recorded individuals under 16 increases faster than others.
Awareness of issues or of risks	Little awareness, according to interviews and most documents from diverse organizations.
Indifference or reaction	Probably mostly due to the ECHR judgement, there is, according to Genewatch, a change in the press and public attitude towards NDNAD and related issues, involving more public debate.
Awareness campaigns/ results	'Reclaim your DNA' campaign launched by Genewatch after the Marper case. People are incited to write to the police and ask for their DNA to be destroyed, if they believe it is kept without justification. According to Genewatch, this campaign has not been really successful so far, and other campaigns will be launched.
Good practises	None
Campaign to be led. On which themes?	
Others	
Conclusions	It took an ECHR judgement for the UK government to admit the illegality of the NDNAD. Even after this judgement, the government is not keen on implementing it soon and entirely. This shows the need for more a priori control of the government: currently, there is no obligation for ICO (UK DPA) authorization or even opinion to set up a government database (a new legislation is however in project). Second important issue raised is the cooperation with other countries, inside or outside the EU, under such conditions.
Recommendations	Strong guarantees should be adopted at EU level especially regarding government use of biometric and genetic data.
Références	- Interview with Terri Dowty, Action for the Rights of the Child Director, London, 10/06/09 - Interview with David Evans, Senior Data Protection Practice Manager, UK Information Commissioner's Office ICO, London, 11/06/09 - Interview with Jim Killock, Open Rights Group Director, London, 11/06/09 - Interview with Helen Wallace, Genewatch Director, London, 11/06/09 - Genewatch website (http://www.genewatch.org)

	- Liberty website (http://www.liberty-human-rights.org.uk) - Action for the Rights of the Child website (http://www.arch-ed.org) - David Mery's blog (http://gizmonaut.net) - National Policing Improvement Agency website (http://www.npia.police.uk) - NPIA response to David Mery's request for information, 12/11/08 (http://gizmonaut.net/foia/2008-12-12_NPIA.pdf) - NDNAD Ethics Group Report 2008 (http://police.homeoffice.gov.uk/ publications/operational-policing/NDNAD_Ethics_Group_Annual_Report) - Home Office NDNAD website (http://www.homeoffice.gov.uk/ science-research/using-science/dna-database/ - Parliament Document on NDNAD 2006 (http://www.parliament.uk/documents/upload/POSTpn258.pdf) - Parliament briefing, 'Retention of fingerprint and DNA data', 13/05/09 (http://www.parliament.uk/commons/lib/research/briefings/snha-04049.pdf) - Home Office consultation on NDNAD after the Marper case (http://www.homeoffice.gov.uk/documents/cons-2009-dna-database/) - ECHR Judgment, Case of S. and Marper v. The United Kindgom, 04/12/08 (http://cmiskp.echr.coe.int/tkp197/view.asp?item=2&portal=hbkm& action=html&highlight=&sessionid=27427778&skin=hudoc-en) - Hansard, in relation to NDNAD (archives of Parliamentary debates, available on the web), most notably: Hansard 29 Sept 2008: Col 354W; Hansard 27 March 2009: Col 771W; Hansard 1 June 2009. T- he Guardian, 'DNA of 37% of black men held by police', 05/01/06 (http://www.guardian.co.uk/world/2006/jan/05/race.ukcrime) - 'Reclaim your DNA' campaign (http://reclaimyourdna.org)

IV. Interpersonal Communications Fact Sheets

IV.1. Communication Data retention

THEME	**Interpersonal Communications**
Identification of technology	**Data Retention**
Technology used/tool (For each teams, a card pro tool)	**Retention of Data during an electronic communication**
Country/ use area	UK
Frame of use	Telecom operators (including Internet service providers) are required to retain communication data for 12 months on their servers, so that government agencies may access them.
Population concerned: target and age	General population, all telecom operators subscribers and users of fixed and mobile telephony, and internet services.
% of users/of young users	Whole population.
Trends (measured / supposed)	The trend for data retention at national level and at the EU level and mutually reinforcing and justifying each other. When the 1997 Directive was in force, telecom operators had the obligation to erase of anonymize communication data after the communication was completed. They could only keep these data for billing and network management purposes. The revision of this Directive in 2002 opened the way for governments to access these data. Further in 2006, the data retention Directive has rendered mandatory the retention of communication data for a period varying between 6 and 24 months. In his annual reports, the UK Interception of Communications Commissioner provides some figures regarding requests for communications data since the entry into force of the related legal provisions. There is a trend showing the increase of such requests, although there is a slight decrease in 2008. Total number of requests by public authorities to 351,243 in 2005; 338,076 in 2006; 519,260 in 2007; 504,073 in 2008. With the new regulation adopted in 2009, these figures will probably get higher.
Known or potentials dangers /Risks	Mass surveillance and profiling of interpersonal communications and networks.
others	
Generated data bases	
Associated data base/ creation (a line pro database)	Telecom operators are required to retain data on their own servers, and respond to public authorities requests on certain data on a case by case basis. The idea of a government centralised database was proposed in 2008 through the so-called 'Interception Modernisation Programme' to facilitate both interceptions and use

	of retained data, as well as to allow for profiling interpersonal communication networks. Following bad press reports and other reactions against 'the Orwellian State', a centralised database has been excluded in 2009 by the government (see below section on legislation). Each telecom operator and Internet service provided thus has its own database.
What justifies the inscription in the file /Risks?	Use of telecom or electronic communication means: fixed and mobile phones, emails, instant messaging, ...
Purposes /contents, main data included / Risks?	Purposes: Billing and network management purposes by telecom operators, plus use by public authorities, as provided by the Data Retention regulations. Content (Data retention Regulations 2009): FIXED NETWORK TELEPHONY Data necessary to trace and identify the source of a communication 1.—(1) The calling telephone number. (2) The name and address of the subscriber or registered user of any such telephone. Data necessary to identify the destination of a communication 2.—(1) The telephone number dialled and, in cases involving supplementary services such as call forwarding or call transfer, any telephone number to which the call is forwarded or transferred. (2) The name and address of the subscriber or registered user of any such telephone. Data necessary to identify the date, time and duration of a communication 3. The date and time of the start and end of the call. Data necessary to identify the type of communication 4. The telephone service used. MOBILE TELEPHONY Data necessary to trace and identify the source of a communication 5.—(1) The calling telephone number. (2) The name and address of the subscriber or registered user of any such telephone. Data necessary to identify the destination of a communication 6.—(1) The telephone number dialled and, in cases involving supplementary services such as call forwarding or call transfer, any telephone number to which the call is forwarded or transferred. (2) The name and address of the subscriber or registered user of any such telephone. Data necessary to identify the date, time and duration of a communication 7. The date and time of the start and end of the call. Data necessary to identify the type of communication 8. The telephone service used. Data necessary to identify users' communication equipment (or what purports to be their equipment)

	9.—(1) The International Mobile Subscriber Identity (IMSI) and the International Mobile Equipment Identity (IMEI) of the telephone from which a telephone call is made. (2) The IMSI and the IMEI of the telephone dialled. (3) In the case of pre-paid anonymous services, the date and time of the initial activation of the service and the cell ID from which the service was activated. Data necessary to identify the location of mobile communication equipment 10.—(1) The cell ID at the start of the communication. (2) Data identifying the geographic location of cells by reference to their cell ID. INTERNET ACCESS, INTERNET E-MAIL OR INTERNET TELEPHONY Data necessary to trace and identify the source of a communication 11.—(1) The user ID allocated. (2) The user ID and telephone number allocated to the communication entering the public telephone network. (3) The name and address of the subscriber or registered user to whom an Internet Protocol (IP) address, user ID or telephone number was allocated at the time of the communication. Data necessary to identify the destination of a communication 12.—(1) In the case of internet telephony, the user ID or telephone number of the intended recipient of the call. (2) In the case of internet e-mail or internet telephony, the name and address of the subscriber or registered user and the user ID of the intended recipient of the communication. Data necessary to identify the date, time and duration of a communication 13.—(1) In the case of internet access— (a)The date and time of the log-in to and log-off from the internet access service, based on a specified time zone, (b)The IP address, whether dynamic or static, allocated by the internet access service provider to the communication, and (c)The user ID of the subscriber or registered user of the internet access service. (2) In the case of internet e-mail or internet telephony, the date and time of the log-in to and log-off from the internet e-mail or internet telephony service, based on a specified time zone. Data necessary to identify the type of communication 14. In the case of internet e-mail or internet telephony, the internet service used. Data necessary to identify users' communication equipment (or what purports to be their equipment) 15.—(1) In the case of dial-up access, the calling telephone number. (2) In any other case, the digital subscriber line (DSL) or other end point of the originator of the communication.
File masters? Risks?	Telecom operators (including Internet Service Providers). Risks are high for the security of data, as well as for misuses of the data by commercial companies.

Who accesses the files/ Sharing of the data base? Access limits? /Risks	As detailed below, access grounds and list of authorized agencies are very large. While access is granted only to senior members of these authorities, this obviously leads to important risks of mass surveillance. Access regulated by law (RIPA). Main access grounds are: (a) in the interests of national security; (b) for the purpose of preventing or detecting crime or preventing disorder; (c) in the interests of the economic well-being of the UK; (d) in the interests of public safety; (e) for the purpose of protecting public health; (f) for the purpose of assessing or collecting any tax, duty, levy or other charge payable to a Government Department. (g) for the purpose, in an emergency, of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health. A large number of government agencies may access communication data under RIPA: - Charity Commission - Criminal Cases Review Commission - Common Services Agency for the Scottish Health Service - a county council or district council in England, a London borough council, the Common Council of the City of London in its capacity as a local authority, the Council of the Isles of Scilly, and any county council or county borough council in Wales - Department for Transport, for the purposes of: o Marine Accident Investigation Branch o Rail Accident Investigation Branch o Air Accidents Investigation Branch o Maritime and Coastguard Agency - a district council within the meaning of the Local Government Act (Northern Ireland) 1972 - Department of Agriculture and Rural Development for Northern Ireland - Department of Enterprise, Trade and Investment for Northern Ireland (for the purposes of Trading Standards) - Department of Health (for the purposes of the Medicines and Healthcare Products Regulatory Agency) - Department of Trade and Industry - Environment Agency - Financial Services Authority - a fire and rescue authority - Fire Authority for Northern Ireland

	- Food Standards Agency - Gambling Commission - Gangmasters Licensing Authority - Government Communications Headquarters - Health and Safety Executive - HM Revenue and Customs - Home Office (for the purposes of the UK Border Agency) - Independent Police Complaints Commission - Information Commissioner - a Joint Board where it is a fire authority - Ofcom - Office of Fair Trading - The Pensions Regulator - Office of the Police Ombudsman for Northern Ireland - Port of Dover Police - Port of Liverpool Police - Post Office Investigation Branch - Postal Services Commission - NHS ambulance service Trust - NHS Counter Fraud and Security Management Service - Northern Ireland Ambulance Service Health and Social Services Trust - Northern Ireland Health and Social Services Central Services Agency - Royal Navy Regulating Branch - Royal Military Police - Royal Air Force Police - Scottish Ambulance Service Board - a Scottish council where it is a fire authority - Scottish Environment Protection Agency - Secret Intelligence Service - Security Service - Serious Fraud Office - the special police forces (including the Scottish Drug Enforcement Agency) - the territorial police forces - Welsh Ambulance Services NHS Trust
Data retention delays/ risks	The delay required by Data Retention Regulations 2009 is 12 months.

Right to be forgotten	
Rights to know or to modify data?	Right to know according to the Data Protection Act. No right to modify.
Covert purposes/ Risks/uncontrolled future evolution	Allows for mapping communications networks. Risks related to the increasing difficulty to differentiate between communication data and content data, especially with new and future communication services.
Others (interconnections…)	
Legislation in application	
Law /rules / others (?) (implemented for this data base or this technology)	The EU Data Retention Directive (2006/24/EC) has been implemented in the UK in April 2009 by a Statutory instrument, the Data Retention Regulations 2009. It requires public communications service providers to retain communications data which they process or generate in the course of their business. Access by public authorities to these data, and oversight of this access, is ruled by the Regulation of Investigatory Powers Act 2000 (RIPA). Before the Data Retention Regulations 2009, data retention was governed in the UK by a system of voluntary data retention, derived from Part 11 of the Anti-Terrorism, Crime and Security Act 2001 (ATCSA).
Risks for freedoms despite the law	The risk for freedoms is related to the general and systematic feature of data retention, in contrast with warranted specific surveillance. With the amount of communication data, the number of providers, the number of government agencies authorized to access the data, and the large grounds for access, real oversight is actually impossible.
If revision of the regulation: reasons? Result: improvement or aggravation (compared to the protection of the DP)	Main reason for the revision in 2009 was the requirement to transpose the EU Data Retention Directive, which was due by 2007. The aggravation is directly related to the aggravation of the legislation in the EU, after the adoption of the Data Retention Directive. Revisions in project: a consultation has been launched in April 2009 by the government ('Protecting the Public in a Changing Communications Environment'), calling for telecom operators to increase the amount of retained data, beyond the EU Directive requirements (retention of third party data, analysis and profiling data). This would require additional legislation. The government justifies its plan by the evolution of the communication environment, including the development of new communication services (most notably VoIP), increase of communication anonymity, the fragmentation of communication data in the future and the issue of jurisdiction as more and more service providers will be based outside of the UK. This consultation document explicitly excludes the creation of a centralized database to store all communication data.
Conformity with the European right (Charter of fundamental rights, directives…)	Conform to EU legislation Directive. The conformity of the Directive itself to ECHR is being challenged in Germany, through the challenge of the national transposition, before the German Constitutional Court. On 10 February 2009 the European Court of Justice decided that the data retention directive was correctly

	adopted on the basis of the EC Treaty as it relates predominantly to the functioning of the internal market. The ECJ was asked by Ireland, supported by Slovakia, to annul the Directive. The privacy issue was not addressed by the ECJ ruling, however, and the main issue of unwarranted registration of the entire population's telecommunications behaviour and movements remains.
Implementation (or not) of the legislation? / Risks	EU Data Retention Directive implemented.
Others	
This tools and young public or young adults	
How far are young people concerned?	Not specifically targeted, but they are concerned to a large extent since electronic communications and instant messaging systems are their preferred modes of communication.
Awareness of issues or of risks	Little awareness. As a 2009 Oxford Institute report shows, UK people concern and attitude towards Internet and privacy has decreased: only 45% agree in 2009 that 'the present use of computers and the Internet is a threat to personal privacy', while they were 66% in 2007.
Indifference or reaction	Privacy watchdogs, other NGOs, Members of Parliament, and the press regularly report about the dangers of data retention.
Awareness campaigns/ results	No specific campaign in the UK.
Good practices	None
Campaign to be led. On which themes?	Campaign on massive surveillance and on the increasing fallacy of the distinction between communication data and content.
Others	
Conclusions	The EU Data retention Directive has been an opportunity to implement or to enlarge data retention at national level. In UK, according to the previous code of practice, the data retention delay for Internet data has been extended from 6 months to 12 months in the course of the transposition of the Directive, which allows for a data retention period comprised between 6 months and 24 months.
Recommendations	Campaign at EU level against Data retention Directive.
References	'The Database State' report (http://www.jrrt.org.uk/uploads/Database%20State.pdf) All Party Parliamentary Group on Privacy (APPG) http://privacyappg.org.uk Home Office Consultation Paper, 'Protecting the Public in a Changing Communications Environment', April 2009 (http://www.homeoffice.gov.uk/documents/cons-2009-communications-data) ECJ Case and ruling, Ireland vs. European parliament, 10/02/09 http://curia.europa.eu/jurisp/cgi-bin/form.pl?lang=EN& Submit=rechercher&numaff=C-301/06 Oxford Internet Institute Report 'The Internet in Britain 2009' (http://www.oii.ox.ac.uk/research/oxis/OxIS2009_Report.pdf)

	Statewatch Document, 'Telephone tapping (and mail-opening figures) 1937-2007 (05/09/08) http://www.statewatch.org/uk-tel-tap-reports.htm Report of the interception of communications Commissioner for 2007 http://www.official-documents.gov.uk/document/hc0708/hc09/0947/0947.pdf Report of the interception of communications Commissioner for 2008 http://www.official-documents.gov.uk/document/hc0809/hc09/0901/0901.pdf

V. Social Networks Usage

V.1. Social networks websites used in the UK

The social networks usage has increased a lot in the past years and UK could not miss the trend. Visiting a social network website is a mainstream activity while online. What might be different from other countries is that the UK has no special social network focusing only on this territory[23], and, probably taking advantage of the language spoken, are using to a large extent the existing social networks available on the Internet.

The major social networks used in UK as indicated by our interviewers[24] were confirmed by a recent study made public by Comscore[25], that positioned Facebook, Bebo and Myspace in the top of the social network websites accessed by the UK users. Our interviewers confirmed that each social network is generally preferred by a special target group, with Facebook being used ussually by middle class and University students, Bebo by teenagers and younger kids and Myspace by artists and other creative teenagers. See below the top 10 as released by Comscore:

Top 10 Social Networking Sites Ranked by Total U.K. Unique Visitors (000)* May 2009 vs. May 2008 Total U.K., Age 15+ - Home & Work Locations Source: comScore World Metrix			
Property	**May-08**	**May-09**	**% Change**
Total U.K. Internet Audience	*34,489*	*36,855*	*7*
Social Networking	*27,118*	*29,444*	*9*
Facebook.com	15,195	23,860	57
Bebo	11,895	8,546	-28
Windows Live Profile	N/A	6,891	N/A
MySpace Sites	8,335	6,531	-22
Twitter.com	80	2,670	3,226
Digg.com	1,311	1,759	34
Friends Reunited Group	3,271	1,629	-50
Tagged.com	669	1,625	143
Deviantart.com	900	1,453	61
Buzznet	939	1,370	46

It is also worth pointing out that the study revealed that 89% of the users between 25-34 years old and 86% of the users between 15-24 visited a social networking site at least one time in the past month. The two groups are the biggest age segments that are using the social networks in the UK.

---

23 The most visited UK- based social network is Badoo.com , but its website is not focused on UK. Its estimated number of users is 19 million.

24 Internews with Terri Dowty - Action on Rights for Children and David Evans, Senior Data Protection Practice Manager at the Information Commissioner's Office ICO – on 10-11.06.2009

25 Nine Out of Ten 25-34 Year Old U.K. Internet Users Visited a Social Networking Site in May 2009 – 20.07.2009, available at http://www.comscore.com/Press_Events/Press_Releases/2009/7/Nine_Out_of_Ten_25-34_Year_Old_U.K._Internet_Users_Visited_a_Social_Networking_Site_in_May_2009

Also it needs to be underlined the huge increase in the usage of micro-blogging, with Twitter.com that grew more than 3,000 percent during the past year to 2.7 million visitors from UK in May 2009.

V.2. Information Commissioner and social networking

The UK Data Protection Authority – the Information Commissioner (ICO) – has launched only at the end of 2007 a section dedicated to young people[26] that also included basic information related to social networking websites & privacy issues.
On this occasion the ICO has made public[27] some results of a research developed by the Commissioner that showed that 71% of the young people (14-21 years old) said that they would not want a college, university or potential employer to conduct an Internet search on them unless they could first remove content from social networking sites. And almost 60% have never considered that what they put online now might be permanent and could be accessed years into the future.
As regards the data that young people make available online, 60% post their date of birth, a quarter post their job title and almost 10% give their home address.
The research also showed a lack of understanding on what data do social networks websites gather from them and how that can be used in order to target advertisement.

ICO has also launched in 2008 a project addressing UK students called Student Brand Ambassador programme.[28] In this project 15 students from universities throughout the UK were recruited. They promoted the key ICO messages on and off campus. The campaign was aimed at alerting students to the risks associated with their personal information and the importance of protecting it. The methods of distributing the information included a Facebook group called "Keep your privates private."

Despite these campaigns, the ICO admitted that from the 25 000 complaints on data protection received in 2008/2009, only a few were dedicated to social networks. The most prominent one was a complaint regarding the deletion of a user profile from Facebook, even after terminating the user's account.

Other public bodies, such as the Home Office Task Force on Child Protection, that gathered representatives of the industry, charity and law enforcement agencies, issued in 2008 a good practice guidance[29] for the providers of social networking and other user interactive services. This document provided advice for industry, parents and children about how to stay safe online.

V.3. Local reactions (Campaigns, cases, etc.)

In a case from 2007 that involved the social networks and its usage by young people, the Student Union at the Oxford University has urged students to change their privacy settings in their account on Facebook, so that the informational they post there is not publicly available. A

---

26 Page available at http://www.ico.gov.uk/youth.aspx
27 See Press release: 4.5 million young Brits' futures could be compromised by their electronic footprint – 27.11.2007 – available at http://www.ico.gov.uk/upload/documents/pressreleases/2007/social_networking_press_release.pdf
28 See ICO Newsletter November 2009 available at http://www.ico.gov.uk/tools_and_resources/enewsletter_and_alerts/previous_enewsletters/English/Edition11.aspx
29 Documents available online at http://police.homeoffice.gov.uk/publications/operational-policing/social-networking-guidance/

spokesperson from the Oxford University confirmed that the senior academic staff who deal with disciplinary matters were looking at public pages on Facebook that were accessible to all members on the Oxford network.

A significant international debate that got the UK civil society involved was related to the change of the Facebook's Terms of Service in the first part of 2009. After the initial terms that "implied that Facebook owned any content posted to the site, even after an account was terminated, forever and ever" were revoked, the major social networking website promised to work with users to develop new terms. In the next period Facebook submitted for public comments two documents that should have replace the Terms of Service: the Facebook Principles and a Statement of Rights and Responsibilities.

The documents were heavily criticized by the UK Civil Society, with a drastic document called „Democracy Theatre: Comments on Facebook's Proposed Governance Scheme"[30] being produced by the a group of the University of Cambridge researchers. The study, that was backed also by the EDRi-member Open Rights Group (ORG) from UK, called the process for revising the terms as "democracy theatre" explaining that "the goal is not to actually turn governance over to users, but to use the appearance of democracy and user involvement to ward off future criticism."

A similar position was taken by the UK-based Privacy International that called[31] the whole process a "massive confidence trick."

The research group at Cambridge has published also other studies regarding the social networks and their privacy features including the way the social networking websites are keeping the photos on their servers, even after the user has deleted them[32] and how the free-market competition between social networking websites has shaped their privacy practices.[33]

30 "Democracy Theatre: Comments on Facebook's Proposed Governance Scheme". Authors: Joseph Bonneau, Soren Preibusch, Jonathan Anderson, Richard Clayton, Ross Anderson - University of Cambridge, Computer Laboratory, 29 March 2009, available at http://www.cl.cam.ac.uk/~jcb82/2009-03-29-facebook-comments.pdf

31 See Privacy International says Facebook vote policy is a "massive confidence trick" , 16.04.2009 http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-564312

32 See Attack of the Zombie Photos – 20.05.2009 by *Joseph Bonneau* http://www.lightbluetouchpaper.org/2009/05/20/attack-of-the-zombie-photos/

33 Study is called The Privacy Jungle: On the Market for Data Protection in Social Networks and was presented to the The Eighth Workshop on the Economics of Information Security (WEIS 2009) , Authors : Joseph Bonneau and Sören Preibusch Paper available at http://preibusch.de/publications/social_networks/privacy_jungle_dataset.htm

VI. Other Fact Sheets

VI.1. Children and Youngster Register Database - ContactPoint

THEME	**Children and Youngster Register**
Identification of technology	**Database**
Technology used/tool (For each teams, a card pro tool)	**ContactPoint**
Country/ use area	UK (England only)
Frame of use	Central National Register for Child and Youngster
Population concerned: target and age	Everyone (citizens and foreign residents) under 18, or under 25 if the youngster has special needs (care leaver or with learning difficulties)
% of users/of young users	According to population. Approximately 11 million people are concerned.
Trends (measured / supposed)	No data yet. Database Launched on May 2009, after 'early adoption' by 17 local authorities in early 2009. But according to Terri Dowty (ARCH), ContactPoint is one main part of a whole interconnected system of databases related to children and youngsters.
Known or potentials dangers /Risks	ContactPoint will store all contacts details of the person and the details of anybody working or in contact with the child (doctors, educators, social workers, etc.). It will work as a central index, with a unique number allowing to access and interconnect different databases. It will be accessible by the police. According to Terri Dowty, while intended to be a tool for child protection and child welfare, ContactPoint will help "identify future criminals".
others	
Generated data bases	
Associated data base/ creation (a line pro database)	ContactPoint Database
What justifies the inscription in the file /Risks?	Mandatory inscription at birth.
Purposes /contents, main data included / Risks?	Purpose: child protection, child welfare. Contents: - name, address, gender, date of birth and a unique identifying number - name and contact details for each child's parent or carer - contact details for services working with a child: as a minimum, - educational settings such as schools and GP practices - contact details for other service providers where appropriate, for example health visitors or social workers; and whether practitioners are lead professionals

	and have undertaken assessments under the Common Assessment Framework (CAF). People providing a sensitive service (defined as those in the fields of sexual health, mental health and substance abuse) are required to seek informed, explicit consents from the child or young person (and their parent or carer where appropriate) before recording their contact details on ContactPoint. Where they are recorded, only an indication of an unspecified service is visible. Informed, explicit consent is also required for care leavers, or for those with learning difficulties to remain on ContactPoint up to the of age 25, to facilitate the transition to adult services. Issue with consent: The Government's Information Sharing Guidance says that children from around the age of 12 can usually give valid consent to allow this personal information to be shared. Risks: the unique identifying number allows for access and interconnection to other databases containing more specific data. Accessibility by the police (youth justice system). Potential risk of future interconnection with the National Identity Register.
File masters? Risks?	UK Department for Children, Schools, and Families (DCSF), 'Every Child Matters' Programme.
Who accesses the files/ Sharing of the data base? Access limits? /Risks	Everyone working with the child (education, health, social care, youth justice and some voluntary organisations). Access upon completion of identity checks, criminal records disclosure, and training. Access is monitored. 'mediated access' (through another authorised user) is possible. All in all, approximately 1 million people would access the register. Risk: since ContactPoint is a centralised index with a unique number, it allows for direct or indirect interconnections of many databases in different sectors.
Data retention delays/ risks Right to be forgotten	From birth until 18. Until 25 for those with special needs, upon consent. Mandatory registration.
Rights to know or to modify data?	According to the Data protection act. The practice in the UK is that one is supposed to be able to exercise the right to information starting from age 12. According to interviews with Terri Dowty and David Evans (ICO representative), this actually results in many cases in denying parents the right to access, "to protect the child privacy". Data are updated by public services (mostly through automatic updates from existing databases).
Covert purposes/ Risks/uncontrolled future evolution	Given the existence of numerous other databases and tools for child profiling and predicting behaviour (e.g. those used by the Youth Justice such as ASSET, a young offenders Assessment Profile, or ONSET, to help identifying risk factors), there are high risks for the use of ContactPoint for policing purposes.
Others	CAF (Common Assessment Framework) is an evaluation tool to check if a child

(interconnections…)	has needs. According to Terri Dowty, it is "an opportunity to look at the whole family and all details on the child. Such assessment is supposed to be made with consent, but when consent is not given, this will impact the level of public service delivered. There are plans to build an E-CAF, in order to hold all the completed assessment forms. The CAF is the main mean of entry into the system. ICS (Integrated Children System, for social workers only) ONSET, and ASSET (Youth Justice board, see above)
Legislation in application	
Law /rules / others (?) (implemented for this data base or this technology)	Children Act 2004, Section 12 (Information databases) Children Act 2004 Information Database (England) Regulations 2007
Risks for freedoms despite the law	As explained above
If revision of the regulation: reasons? Result: improvement or aggravation (compared to the protection of the DP)	No revision yet.
Conformity with the European right (Charter of fundamental rights, directives…)	The scheme is rated as 'red' in the 'Database State' report, which means that the concerned database is 'is almost certainly illegal under human rights or data protection law and should be scrapped or substantially redesigned.
Implementation (or not) of the legislation? / Risks	N/A
Others	
This tools and young public or young adults	
How far are young people concerned?	Everyone under 18, or under 25 in special cases. Nationals and foreign residents.
Awareness of issues or of risks	Very low.
Indifference or reaction	According to Terri Dowty, the database has led to "no scandal".
Awareness campaigns/ results	Campaigns from ARCH and the NO2ID Coalition.
Good practises	None
Campaign to be led. On which themes?	Awareness campaign towards children, youngsters and their families. Awareness campaign towards child carers (educators, social workers, health sector)?

Others	
Conclusions	ContactPoint and related databases and programmes are the perfect illustration of the trend (in UK as well as in other countries) to profile and predict children and young people behaviour, including by police and justice services. The delivery of essential public services is a vehicle used for such purposes.
Recommendations	Need for better guarantees (at EU level?) and special protections of children and youngster privacy. Need for guarantees on very restricted use of national unique numbers and registers.
References	Interview with Terri Dowty, Action for the Rights of the Child Director, London, 10/06/09 Interview with David Evans, Senior Data Protection Practice Manager, UK Information Commissioner's Office ICO, London, 11/06/09 UK Department for Children, Schools, and Families, ContactPoint website website http://www.dcsf.gov.uk/everychildmatters/strategy/ deliveringservices1/contactpoint/contactpoint/ BBC News, 'Database of all children launched', 18/05/09 http://news.bbc.co.uk/2/hi/uk_news/education/8052512.stm Action on Rights for Children (ARCH) website http://www.archrights.org.uk/ 'Protecting the Virtual Child – the law and children's consent to sharing personal data', ARCH Report, January 2009 http://www.archrights.org.uk/docs/NYA(4)arch_16.2.0[2].pdf ARCH web page on children databases http://www.archrights.org.uk/issues/databases/childrens_databases.htm FIPR, 'The Database State' Report, March 2009 (http://www.jrrt.org.uk/uploads/database-state.pdf) NO2ID campaign website (http://www.no2id.net) Community Care, 'Information sharing: does new IS system go too far?', 11/02/09 http://www.communitycare.co.uk/Articles/2009/02/11/110654/ contactpoint-practitioners-harbour-doubts.html