The EDRi papers
EDITION 02

EU SURVEILLANCE

A summary of current EU surveillance and security measures

EUROPEAN DIGITAL RIGHTS

The purpose of this booklet is to briefly outline current EU surveillance and security measures in order to give an insight into their scale and cumulative effect.

In order to be legal under the EU Charter of Fundamental Rights and the European Convention on Human Rights, each security measure that limits fundamental rights is understood to be effective and a “necessary” and “proportionate” breach of the rights which our society considers to be fundamental.

CONTENTS:

Booklet written by:
Joe McNamee, Advocacy Coordinator
Kirsten Fiedler & Marie Humeau, Advocacy Managers & Daniel Dimov, intern

With special thanks to Statewatch for valuable expert input to this document.

Design by: CtrlSPATIE

Photography by: Marnix Petersen

European Digital Rights (EDRi) is an association of 28 privacy and digital civil rights associations from 18 Countries.

European Digital Rights
39 Rue Montoyer
B-1000 Brussels
tel: + 32 (0)2 550 4112
brussels@edri.org

EXECUTIVE SUMMARY

Once adopted, security measures are notoriously difficult to repeal – regardless of their impact on freedoms, unintended consequences and effectiveness. Security and freedom are not contradictory priorities that need to be balanced – security is a key element of our freedom. If security is being balanced against freedom, it is no longer fulfilling its role.

These questions need to be asked now because of the radical increase in surveillance during the last decade, with the cumulative effect of parallel developments rarely discussed.

Imagine, for instance, that you need to fly to another country. In order to book your ticket, a phone call is made to the travel company. Even when there is absolutely no grounds for suspicion of wrong-doing, in all cases, the following tracking will be undertaken:

Under the Data Retention Directive (Directive 2006/24/EC), details of the phone call will be recorded (including the physical location of the citizen), and stored for up to two years.

When buying a flight ticket, under the proposed Passenger Name Record (PNR) Directive and bilateral agreements, data ranging from credit card details to what you have chose to have for lunch are stored, communicated nationally and internationally and automatically processed in order to profile citizens as possible terrorists or people-traffickers.

If a bank transfer is used to pay for the ticket, the data relating to the transaction will be retained for five years under EC money laundering Directives. It may then subsequently be shared with the USA under the dedicated Terrorist Financing Tracking Programme (TFTP), or bilaterally, through the informal Egmont group of 116 Financial Intelligence Units across the world.

Then, on the way to or at the airport a host of surveillance technologies being developed under the €1.4 billion EU security research programme may be used to analyse the movements, behaviour, profile, physical characteristics or belongings of the traveller.

When you finally get to the airport, your body may be scanned, as the fifth privacy intrusion involved in buying a ticket and taking a flight.

ON YOUR WAY TO THE AIRPORT?

The **SECUR-ED** project, led by French defence giant Thales has received €25.5 million in EU funding to demonstrate a range of surveillance and detection technologies on transport networks in Madrid, Paris, Milan and Berlin. http://www.secur-ed.eu/

The **PROTECTRAIL** project, led by a subsidiary of the Italian defence giant Finmeccanica, has received over €13 million in EU funding to develop integrated surveillance systems covering entire rail transport networks http://protectrail.eu/.

The €2.5 million **SAMURAI** project uses cameras that watch and learn to detect "suspicious and abnormal behaviour" in airports and other public places http://www.samurai-eu.org/.

The **TASS** project – Total Airport Security System – is led by Israel's Verint Systems. It's consortium has received €9 million in EU funding to develop 'next generation' airport intelligence systems. http://www.tass-project.eu/

The **EFFISEC** project led by Morpho (the French security and defence company formerly known as Sagem), has received €10 million in EU funding to develop the "security checkpoint of the future" by integrating biometric identification systems with substance detection and video surveillance technologies. http://www.effisec.eu/

DATA RETENTION

WHERE ARE YOU AND WHO ARE YOU IN CONTACT WITH?

The Data Retention Directive (Directive 2006/24/EC) was adopted as a reaction to the London bombings in 2005 (even though data retention would have had no effect at all in that tragedy).

It was proposed as a result of lobbying by the British police on the UK government and was pushed through by the UK Presidency of the Council in the second half of 2005. The European Parliament approved the Directive despite the Civil Liberties Committee having repeatedly confirmed that untargeted data retention is an unnecessary restriction on the fundamental rights of citizens.

Did you know?

The Directive or its implementation has been ruled illegal by the courts in the Czech Republic, Cyprus, Germany and Romania and Ireland is going to refer to the European Court of Justice on that matter.

The Directive requires providers of fixed and mobile telephony and internet services to retain details of the communications, including the physical location (for mobile operators), of all citizens – even those never suspected of committing a crime – for 6- to 24-month periods.

A Single Market Directive? The Directive contains the safeguard that the data collected can only be used to fight "serious crime", but the absence of a definition of "serious crime" in many Member States renders this meaningless.

The Directive requires operators to supply the data to the "competent national authorities". When normally "competent authorities" are judicial, they include tax/customs authorities in six Member States, border authorities in three Member States and public authorities in one Member State.

Access to the data requires judicial authorisation for every access in eleven Member States, it is required in "most" cases in three Member States, a "senior authority" but not a judge gives authorisation in four Member States. In two Member States, the only safeguard is that requests for access need to be made "in writing".

The retention period is the same for both Internet and telephony data in fifteen Member States, ranging from 6 months in Cyprus, Lithuania and Luxembourg to 2 years in Poland. The remaining Member States retain different types of data (fixed, mobile, Internet and failed connections) for different periods of time.

PASSENGER NAME RECORD

WHO ARE YOU AND WHERE ARE YOU GOING?

Passenger Name Record (PNR) is a record of the information necessary to enable reservations to be processed by travel agents and airlines – plus additional data now required by governments.

As some PNR data is regarded to be useful in some investigations, PNR will now also be extended and reused to be processed, stored for years and used in the profiling of all travellers as potential criminals.

That data is available to governments and travel agencies around the world and ranges from predictably useful data such as frequent flyer information and credit card details to more bizarre information such as meal preferences.

In 2011, the European Commission published a legislative proposal requiring airlines to transfer PNR data to national authorities in all Member States, who will use these data for investigation and prosecution of "serious crimes" – this processing will include profiling of innocent citizens based on unknown and unpredictable criteria.

The scope of the proposed Directive covers:

- transfer, process and retain PNR data of passengers flying into or out of the EU.
- Potential extension of the scope of the Directive: after four years, the Directive may cover PNR data of passengers on

"PNR will now also be extended and reused to be processed, stored for years and used in the profiling of all travellers as potential criminals"

"European Parliament has approved the EU/ Australia agreement despite the European Commission failing to included the minimum safeguards"

flights internal to the EU, this has already been demanded by some Member States.

- Each Member State would be required to establish a surveillance authority to undertake the profiling activities and the forwarding of passenger data to third countries.

- The main task of the surveillance authorities is to programme and review automatic decisions based on PNR data in order to approve the computer's guesses as to whether individual and previously unsuspected citizens are involved in terrorist activities or serious transnational crimes.

- PNR data may be transferred to non-member states and then onwards to third countries, with no meaningful controls.

- PNR data should be retained by the authorities for 30 days after the time when the international flight arrives or departs. Thereafter a fiction of "partial anonymisation" is used, after which data is retained for 5 years (EU, EU/Australia) or 15 years (2011 EU/US proposal).

The European Parliament has approved the EU/Australia agreement despite the European Commission failing to include the minimum safeguards, that it had previously demanded to be the minimum to protect the fundamental rights of innocent travellers.

EUROPOL'S INTELLIGENCE FILES

WHAT DOES EUROPOL'S COMPUTER SYSTEM DO?

Europol (short for European Police Office) is the European Union's criminal intelligence agency that aims to improve the effectiveness and co-operation between the competent authorities of the Member States primarily by sharing and pooling intelligence to prevent and combat serious international organized crime. EUROPOL is allowed to collect and store information on crimes and alleged crimes, and people convicted or suspected of these offences.

Europol has a comprehensive information system, the so-called Europol Computer Systems (TECS) which has three components:

- The Europol Information System (EIS) is intended to record "hard" data of Member States on crimes and perpetrators. The EIS is currently being developed, and Europol is testing an initial version focusing on currency counterfeiting. All relevant data - including personal data - is being passed on by national police authorities.

- The Index System provides a search function, which refers to the contents of the Analysis System.

- The Analysis Working Files (AWF) can include actual and potential suspects, witnesses, victims, contacts, associates and informants; suspected and alleged offences; modus operandi and suspected membership of a criminal organisation; convictions, and references to investigations by national police forces. The circle of people that can be recorded is thus potentially limitless. Controversially, and in derogation of Council of Europe standards on police data, the AWFs may also include sensitive information on political or sexual orientation etc.

- The 21 AWFs are currently being reorganised and are likely to be merged into a few larger files. The US has already applied for access to some of them.

Warehousing European police and immigration data

On 12 September 2011, the Council adopted a regulation for the establishment of a European "Agency for the operational management of large-scale IT systems in the Area of Freedom, Security and Justice". It will enter into operation in summer 2012.

The agency is going to manage Schengen Information System II (SIS II), the Visa-Information System (VIS) and EURODAC.

The SIS is a governmental database that is currently used by 27 European countries to record the details of millions of people. A revision of this database is currently under development. The SIS II will provide new functionalities including the addition of biometric identification data (photographs and fingerprints); new categories ("terrorist suspects", "violent troublemakers") and the linking of individual records. It has been suggested to transform it into a system of investigation, thus modifying its original finality of a check tool.

The VIS went live in 2011 and contains information, including biometric identification data, on visa applications by Third Country Nationals requiring a visa to enter the Schengen area. The system will "contribute to the prevention of threats to the internal security of any of the Member States".[01] It is expected to contain some 70 million biometric records at full capacity and will share a "common technical platform" with SIS II.

EURODAC is the European fingerprint database for identifying asylum seekers. Asylum applicants and irregular border-crossers over the age of 14 have their fingerprints taken. All EU Member States currently participate in the scheme, plus three additional European countries: Norway, Iceland and Switzerland. End of 2003, EURODAC contained 1.3 million fingerprints.

It was already suggested that this IT agency could develop the EU Terrorist Finance Tracking Programme (TFTS) and a passenger surveillance and profiling system for European passenger name records.

In an opinion issued on 7 December 2009, EPDS Peter Hustinx showed his concern related to the expansion of the agency powers:

"The total number of large-scale IT systems managed by one and the same Agency should therefore be restricted to a number with which the data protection safeguards can still sufficiently be assured. In other words, the point of departure should not be to bring as many large-scale IT- systems as possible under the operational management of one Agency."

FINANCIAL RECORDS

WHO PAID WHAT, TO WHOM AND WHEN?

EC money laundering directives impose 'customer due diligence and record-keeping' obligations on financial institutions, intermediaries and other designated non-financial businesses and professions, requiring the keeping of accounts and transactional records for at least five years.

The 1991 Directive (91/308/EC) assumes that any unexplained transaction of €15,000 (or several transactions totalling €15,000 that seem to be linked) is 'suspicious' and obliges member states to ensure that the employees of credit and financial institutions: "cooperate fully with the authorities... by informing [them], on their own initiative, of any fact which might be an indication of money laundering" or terrorist financing and "by furnishing those authorities, at their request, with all necessary information". All EU member states have established Financial Intelligence Units (FIUs) to process Suspicious Transactional Reports (STRs), assist police investigations requiring financial information and share information at EU level.

Did you know?

The European Data Protection Authorities, united in the Article 29 Working Party, is not convinced on necessity and proportionality of the proposal for European Terrorist Finance Tracking System. In October 2011, the Article 29 Working Party called upon the Commission to present evidence for its necessity and proportionality.

The United States' Terrorist Finance Tracking Programme (TFTP) includes an agreement with the EU known as the SWIFT agreement which allows US authorities to request and, upon the approval of Europol (not impartial as it can thereafter also gain access), large volumes of transaction information from the Society for Worldwide Interbank Financial Telecommunication (SWIFT) to the United States. SWIFT is an inter- service banking company that is used in roughly 80 percent of international transactions. The agreement came into force in the summer of 2010.

The agreement, due to concerns about proportionality, transparency and fundamental rights, was endorsed with reluctance by MEPS, who initially vetoed it in February 2010. They were rewarded with some essentially meaningless concessions, including a specially appointed, anonymous EU representative to oversee the transfer of the data and the inclusion of Europol who would approve requests for data, instead of the independent oversight body they had asked for.

An inspection report published by Europol in March 2011 found that the US requests were too general and too abstract to allow proper evaluation of the necessity of the requested data transfers. The inspection also revealed a lack of audit of the data transfers. However, none of the unverifiable requests were rejected.[02] The EU is currently discussing the establishment of a dedicated European TFTP from which data would be exchanged with the USA and other states.

SURVEILLANCE SUBSIDIES

THE EU SECURITY RESEARCH PROGRAMME (ESRP)

The European Security Research Programme is a €1.4 billion component of the current seven-year, €51 billion EU Framework Research Programme (FP7, 2007-13).

The ESRP has the twin objectives of enhancing public safety through the development of security technologies and fostering the growth of a globally competitive European 'Homeland Security' industry. Unlike other aspects of FP7, the ESRP is managed by the European Commission's DG Enterprise rather than DG Research. A significant increase in security research funding is expected in the Horizon 2020 programme to be debated in 2012.

Many of the projects funded to date concern surveillance technologies. This includes internet, telecommunications, financial and social network surveillance; 'smart' CCTV; risk profiling and behavioural analysis; tracking and identification systems; nanotech and biotech applications; virtual fences; drones/UAVs, earth observation and satellite tracking; and automated targeting systems, to name but a few. Although the then UK Prime Minister Tony Blair, admitted after the bombing of the London transport network that "all the surveillance in the world" could not have prevented the attacks,[03] there is no limit to the technological controls envisaged by the architects of the ESRP.

Did you know?

The agenda for the ESRP has been strongly influenced by representatives of corporations from the defence and security industries.

Successive advisory bodies established by the European Commission (the Group of Personalities, European Security Research Advisory Board and European Security Research and Innovation Forum) have all been dominated by industry stakeholders and perspectives. Research commissioned by the European Parliament, published in November 2010,[04] found that "representatives from civil society and parliamentarians, as well as bodies and organisations in charge of civil liberties and fundamental freedoms, including data protection authorities and fundamental rights bodies, have been largely sidestepped. The outcome of this process is a dialogue that is limited in its scope, addressing security research through the concerns of security agencies and services and the industry, without taking into account the requirements flowing from the EU's internal area of freedom".

The report analysed the first 91 ESRP projects, worth a total of €443,2 million, and found that "companies such as the Thales group are involved in roughly one third of the projects (27), representing more than half the FP7-ST (57%) in terms of projects' total worth (€ 253.8 million)".

SMART METERS

WHAT CAN YOUR TV SAY ABOUT YOU?

Smart meters measure the consumption of gas and electricity. They can be integrated in a smart grid, a network of users and producers that ensures better tuning of supply and demand.

Even though it has been demonstrated that smart meters can be implemented with no privacy concerns whatsoever,[05] all implementations currently underway ignore basic principles of "privacy by design" and raise significant privacy and security concerns. These issues are particularly important because the European Union decided that 80% of all users are to have a smart meter in 2020.[06]

Issues raised by the smart meters:

- Privacy: The proposed implementations needlessly create additional resevoirs of personal and sensitive data. Governments, electricity producers and/or others may gain access to detailed information about our energy use and can be used for profiling purposes. It is inevitable that this data will be sought by governments, marketers and by criminals, for whom this information would be equally valuable.
- Security: The total failures of current plans regarding the security of personal data do not inspire confidence regarding the wider security precautions in future vv. The dangers of weak security leading to consumer networks being hacked are very evident.

Did you know?

German researchers (Data Privacy Management) discovered in September 2011 that smart meters can even determine which programmes consumers are watching on a standard TV set by analysing electricity consumption patterns.[07]

BIOMETRIC DATA

RECORDING EYES, FINGERS, DNA

On December 13, 2004, the EU Council passed the Regulation 2252/2004 on standards for security features and biometrics in passports and travel documents issued by the Member States.

As a result, Member States are increasingly demanding storage of biometric data (such as facial scans or fingerprints in interoperable formats) of their citizens. The data is then stored on 'RFID' chips in national passports and ID cards. Some governments additionally store these biometric data in databases.

The Regulation also foresees that the biometric data should be secured and the storage medium shall have sufficient capacity and capability to guarantee the integrity, the authenticity and the confidentiality of the data.

Biometrics will also be increasingly extended to other aspects of social life. The European Parliament had severe doubts about the introduction of such measures, but agreed to their introduction in very questionable circumstances.[08]

The EU's Joint Research Centre expressed the hope that "once the public becomes accustomed to using biometrics at the borders, their use in commercial applications will follow. The large-scale introduction of biometric passports in Europe provides a unique opportunity... Firstly, the creation of a demand market based on user acceptance... Second, the fostering of a competitive supply market."[09]

The EU's Schengen Information System II, which contains the details of millions of people wanted, missing, under surveillance or expelled from the EU, has introduced biometrics into individual SIS records. The European Commission is now working on a package of 'e-borders' proposals, including an 'entry-exit' system that would record movements into and across the EU and share the SIS II's biometric platform.

Did you know?

There is no such thing as secure data. In Germany, the newly introduced biometric e-IDs have been already hacked several times.[10]

Illegal access to the stored data would indeed be useful to create new passports or hijack identities for supposedly secure transactions online.

PRINCIPLE OF AVAILABILITY

A 'SELF-REGULATED' 'FREE MARKET IN PERSONAL DATA'

The Hague Programme established the so-called "principle of availability". It was neither subject to parliamentary scrutiny by national or European parliaments nor was it available to civil society before it was adopted.

The Commission did not put forward its formal proposal[11] for a Council Decision on the "principle of availability" until after the Prüm Treaty[12] and just two weeks before the "Friends of the Presidency" (FoP)[13] report.

For the law enforcement agencies, information exchange procedures often take too much time, involve formal requests and sometimes judicial authorisation. The aim of the principle is therefore to facilitate cooperation between the police and judicial authorities of the EU's Member States and "that as large a list of information categories as possible is exchangeable with as little effort as possible (ie: requiring a minimum of formalities, permissions, procedures, if any)".[14] However, while this process has been moving forward continuously, data protection in the area of police and judicial cooperation has failed to keep pace.

The principle of availability and the "free market" in access to all national and European Union databases is a perfect

"The free market in access to data/ intelligence will rely on 'self-regulation' by the law enforcement agencies and make accountability almost meaningless"

example of how the fight against terrorism has increased powers of surveillance and control, without, at the very least, the controls and legal protections required under the Lisbon treaty.

Law enforcement agencies will be more and more "self-regulated" with all of the dangers of misuse and abuse that this entails. The police, immigration, customs and security agencies will have unfettered access to any data held within the EU and, as is increasingly hinted at, with "friendly" non-EU states too.

'The free market in access to data/ intelligence will rely on "self-regulation" by the law enforcement agencies and make accountability almost meaningless'.[15]

Implementing the Principle of Availability

Cooperation between Member States and access to national and EU databases has increased significantly in the last decade. The following systems stem from demands for a greater degree of information exchange and co-operation between the law enforcement authorities:

- The European Criminal Records Information System (ECRIS) is a database that enables Member States to share the criminal records of their citizens. It is marked by serious gaps in data protection,[16] a reliance on potentially untrustworthy automated translation, and a significant lack of oversight. It is currently estimated that 100,000 messages per month will be exchanged via the system.

- The European Commission and a small group of Member States insisted on the establishment of the EPRIS (European Police Records Index System) and is currently being discussed by the Council and the European Parliament. Its aim is to provide national police forces with the ability to search each others' databases, to find out if and where information on individuals can be found.

- The Information Exchange Platform for Law Enforcement Authorities (IXP) proposes to centralise access to all the EU's law enforcement information exchange instruments. Its development is still in the early stages, but a suggestion extending access to the European Union's bureaucracies including to a number of Directorate Generals of the European Commission, and the General Secretariat of the Council[17] – would appear to be a breach the fundamental principle of "separation of powers" between the lawmakers and the law enforcement agencies (whose job is to implement the law).

- Although EPRIS and the IXP might become serious issues in the near future, of current concern are the implementation of the "Prüm Decisions" networking national police databases (fingerprints, DNA and vehicle registers) and of the "Swedish Initiative" meant to accelerate information exchange between law enforcement agencies with tools for a semi-automated data transfer already under development.

BODY SCANS

EVERYBODY'S PRIVACY?

A full body scanner is a device that is theoretically able to detect contraband that may be hidden under someone's clothing. The scanner creates a full 3D image of a person including detailed body contours.

These types of scanners are privacy-invasive in many ways:

- Governments do not have the right to make strip searches routine and mandatory, regardless of whether it is done by physically removing clothes or by using other, technological means.
- Body scans allow screeners to see the nude surface of the skin. This can allow the security staff to see if the person is carrying concealed objects, but it is far from clear that the success level of the equipment is worth the damage to human dignity.
- Finally, much of the controversy centers around the fact that it is possible for the data images taken by the scanners to be abused. Concern has particularly been focused on the potention for abuse in images of celebrities, children and women.

On 6 July 2011, the European Parliament adopted a resolution and took a number of these concerns into account. According to the MEPs, passengers should have the right to refuse body scanning and opt for alternative screening methods that guarantee the same level of effectiveness while respecting their rights and dignity. Such a refusal should not give rise to any suspicion of the passenger. To protect human dignity, privacy and intimacy, only stick figures should be used and no body images may be produced. Finally, the data must be destroyed right after the person has passed through the security control and the technology used must not even have the capabilities to store or save data.

Despite all efforts by the European Parliament, body scans still cannot be justified. Privacy infractions remain and will occur on an enormous scale, every single day. Experts even doubt their overall effectiveness (e.g. hiding illegal substances in body cavities could probably get around the scans quite easily).

NOTHING TO HIDE, NOTHING TO FEAR?

IT IS NOT THAT SIMPLE

#1 News International – a multinational company that hacked phones (including that of a missing child) to gain information for stories has publicly admitted to paying police officers for data.[18]

#2 A female Irish police intelligence officer tapped her ex-boyfriend's phone and accessed data retained under the Data Retention Directive.[19] She now works in the anti-terrorism unit of the Irish police force.

#3 German telecommunications giant Deutsche Telekom illegally used telecommunications traffic and location data to spy on about 60 individuals including critical journalists, managers and union leaders in order to try to find leaks. The company used its own data pool as well as that of a domestic competitor and of a foreign company.[20]

#4 In Poland retained telecommunications traffic and subscriber data was used in 2005-2007 by two major intelligence agencies to illegally disclose journalistic sources without any judicial control.[21]

#5 The Irish data protection authority is currently investigating complaints of Irish police abusing the national police database to run background checks on people their family members are involved with and checking vehicle histories. This comes from a 2010 report from the data protection authority which complains that "despite our repeated engagements on this issue, the monitoring of access by members of An Garda Síochána [the police force] to Pulse [the national database] falls short of the standards we expect".[22]

#6 On 19 August 2009, a flight from Paris-Charles de Gaulle to Mexico City was refused permission to cross over the US, and diverted in mid-flight. The US refused to allow one of the passengers, Paul Emile Dupret, a Belgian citizen and trade policy analyst on the staff of the GUE/NGL group in the European Parliament, to enter US airspace. On a previous trip M. Dupret had been detained and interrogated, despite being part of an official European Parliamentary delegation, during a scheduled refueling stop in Miami on a through Iberia flight from Caracas to Madrid.[23]

NOTES

01 Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation), Recital 5

02 http://europoljsb.consilium.europa.eu/media/112160/jsb%20tftp%20inspection%20-%20website%20notice,%20march%202011.pdf

03 We cannot stop these attacks, says Blair", The Telegraph, 8 July 2005, http://www.telegraph.co.uk/news/1493695/We-cannot-stop-these-attacks-says-Blair.html

04 http://www.statewatch.org/news/2010/nov/ep-review-security-research- programme.pdf

05 http://research.microsoft.com/en-us/projects/privacy_in_metering/

06 http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/mission.pdf

07 http://www.its.fh-muenster.de/greveler/pubs/smartmeter_sep11_v06.pdf

08 http://www.statewatch.org/news/2004/nov/12biometric-passports- blackmail.htm

09 http://www.statewatch.org/news/2005/mar/17eu-biometric-report.htm

10 http://www.thelocal.de/sci-tech/20100824-29359.html and http://www.heise.de/newsticker/meldung/Weitere-Sicherheitsluecke-beim-elektronischen- Personalausweis-1319432.html

11 COM(2005) 490 final http://eur-lex.europa.eu/LexUriServ/LexUriServ.do? uri=COM:2005:0490:FIN:EN:PDF

12 The Prüm Treaty was signed in secret governmental meetings to develop cross- border cooperation in combating terrorism, illegal migration and cross-border crime.

13 The FoP group of experts from the member states plus the General Secretariat of the Council and the Commission was set up in April 2005 to develop the "technical modalities to implement the Principle of Availability" http://register.consilium.europa.eu/pdf/en/05/st13/st13558.en05.pdf

14 EU doc no: 7416/05

15 Tony Bunyan, Statewatch, December 2006. The "principle of availability" http://www.statewatch.org/analyses/no-59-p-of-a-art.pdf

16 http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Pres sNews/Press/2008/EDPS-2008-09_ECRIS_EN.pdf

17 Council of the European Union, Business Concept for an Information Exchange Platform for Law Enforcement Agencies, 1117/10, 15 June 2010, p.2 http://register.consilium.europa.eu/pdf/en/10/st11/st11117.en10.pdf 17 http://www.guardian.co.uk/media/2011/mar/30/mps-ask-rebekah-brooks-sun-payments-to-police

18 http://www.guardian.co.uk/media/2011/mar/30/mps-ask-rebekah-brooks-sun- payments-to-police

19 http://www.tjmcintyre.com/2011/02/judges-report-reveals-allegations-that.html

20 http://www.spiegel.de/international/business/0,1518,556741,00.html

21 http://wyborcza.pl/1,75478,8842563,Inwigilacja_dziennikarzy_badana_od_now a.html

22 http://www.edri.org/edrigram/number9.17/abuses-irish-police-databases

23 http://www.spectrezine.org/resist/Dupret.htm

Last modified on: 23 January 2012 12:43

EDRI.ORG/PAPERS

With financial support from the EU's Fundamental Rights and Citizenship Programme.