Defying the logic, forgetting the facts: the new European proposal for data protection in the police sector

Joseph A. Cannataci[1]

Cite as: Cannataci, J.A., "Defying the logic, forgetting the facts: the new European proposal for data protection in the police sector", in European Journal of Law and Technology, Vol. 4, No. 2, 2013.

Abstract

The European laws surveilling surveillance may possibly soon become more complex or more uncertain, depending on developments during the next 12-36 months. On the 25th January 2012 the European Commission published two, not one, proposals for new legislation in the ever-growing field of privacy and data protection. One of these two proposals is the mildly-named but potent "Regulation" covering most sectors of activity except for the law enforcement and criminal justice sectors which are proposed to be governed by a separate Directive. Both the Article 29 Working Party and the European Data Protection Supervisor in March 2012 overall welcomed the Draft Regulation, whereas they strongly criticised the Draft Directive which is regarded as being greatly inferior to the Draft Regulation. This level of criticism begs a number of important questions: why is the police and justice sector being handled differently and separately from other sectors? Why does the current (1995) data protection directive allegedly lead to fragmentation to the extent that in 2012 the Commission proposes a Regulation to replace it yet at the same time, almost in the same breath, in 2012 and still in 2013, it is proposing that the Police and Criminal Justice sector be regulated by a Directive? Would the new Directive on Police use of personal data not produce the same level of fragmentation as the old 1995 Directive did in other sectors? Is this not inconsistent? This paper examines whether these new laws are fit-for-purpose by first laying out the realities that the law must presumably set out to regulate. It then examines the problems with the logic and indeed the credibility of some answers provided publicly by the European Commission. After dealing with the logical inconsistencies implicit in the current approach, the paper questions the usefulness of the Draft Directive from a substantive point of view and especially in the wake of the Snowden revelations about the modalities of surveillance being employed world-wide. Utilising summary findings from the PUPIE project, this paper makes the point that, in fact, most of the principles of the Draft Directive are already provided for in the laws of many EU member states so the degree of legislative innovation being proposed is questionable, the harmonization benefits may be minimal, while the allegedly undesirable fragmentation will remain. The paper then traces how, since May 2013, the European debate on data protection was overtaken by,and now benefits from, the revelations made by Edward Snowden. It demonstrates the relative legal impotence of the EU in such matters on account of the fact that matters of national security are reserved to national governments by virtue of Article 4 (2) of the EU Treaty. After analyzing the relevant developments to end October 2013 the paper concludes that the most suitable, and possibly - though not necessarily - the most likely option to European policy-makers is that of pushing for a new Council of Europe convention on Cyber-Security in an effort to balance the privacy and security interests inherent to a debate about surveillance.

[1] J. A. Cannataci is Chair in European Information Policy & Technology Law at the Faculty of Law of the University of Groningen, The Netherlands, Head of Department of Information Policy & Governance, Faculty of Media & Knowledge Sciences, University of Malta and Adjunct Professor at the Security Research Centre, School of Computer and Security Science at Edith Cowan University Australia. (corresponding author phone +356 99 42 61 33 e-mail J.A.Cannataci@rug.nl , Joseph.Cannataci@um.edu.mt and j.cannataci@ecu.edu.au)

"The joint statement from Facebook, Twitter, Microsoft, Google and Yahoo! also contains a plea for the government not to introduce any more legislation on access to communications data until it has considered reforming international treaties that govern surveillance and law enforcement."

The Guardian 18 October 2013

The objective of this study is to examine whether the current Data Protection Reform Package[2] (DPRP) proposed for the European Union (EU) is "fit-for-purpose", trying to dissect available evidence of political posturing, horse-trading and any resultant legal nonsense. The definition of "fit-for-purpose" is crucial: does this mean "fit for the stated purposes", "fit-for-the-unstated purposes" and, most importantly, "fit for the purpose of adequately regulating the current realities and addressing the concerns of policy-makers and citizens alike". The paper will examine some examples taken from each of these three categories of "purpose" and, hopefully fittingly so, because in data protection law the notion of "purpose" has in many ways been a fundamental principle for over forty years. The DPRP is a vast and ambitious project and it would be beyond the scope of this paper to attempt an overall assessment of the entire package. The focus of this paper will therefore at the very outset be limited to the sector of the processing of personal data by police and similar Law Enforcement Agencies (LEAs) as well as Security & Intelligence Services (SIS). The study will first outline fourteen basic facts concerning the realities of the situation in autumn 2013 on the assumption that if the existing or new laws do not provide adequate safeguards for all of these basic facts then they cannot be declared to be truly fit for purpose. A distinction will be made between "fit for purpose" when considered in the light of the known facts and being "an improvement" for the citizen and all the actors involved then. The discussion of facts will then give way to an evaluation of risk arising out of some of the facts previously highlighted. Once a number of facts and risks are identified, the study will then focus on the adequacy of the proposed legislation to deal with these facts and the associated risks. This is such a fast-moving field that the reader is kindly asked to note the date and version of this study[3] since things may have changed significantly since its publication.

---

[2] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) Brussels, 25.1.2012 COM(2012) 11 final 2012/0011 (COD)

Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data /* COM/2012/010 final - 2012/0010 (COD) */

[3] Version 4c Tuesday 29 October 2013 at 23h00 CEST.

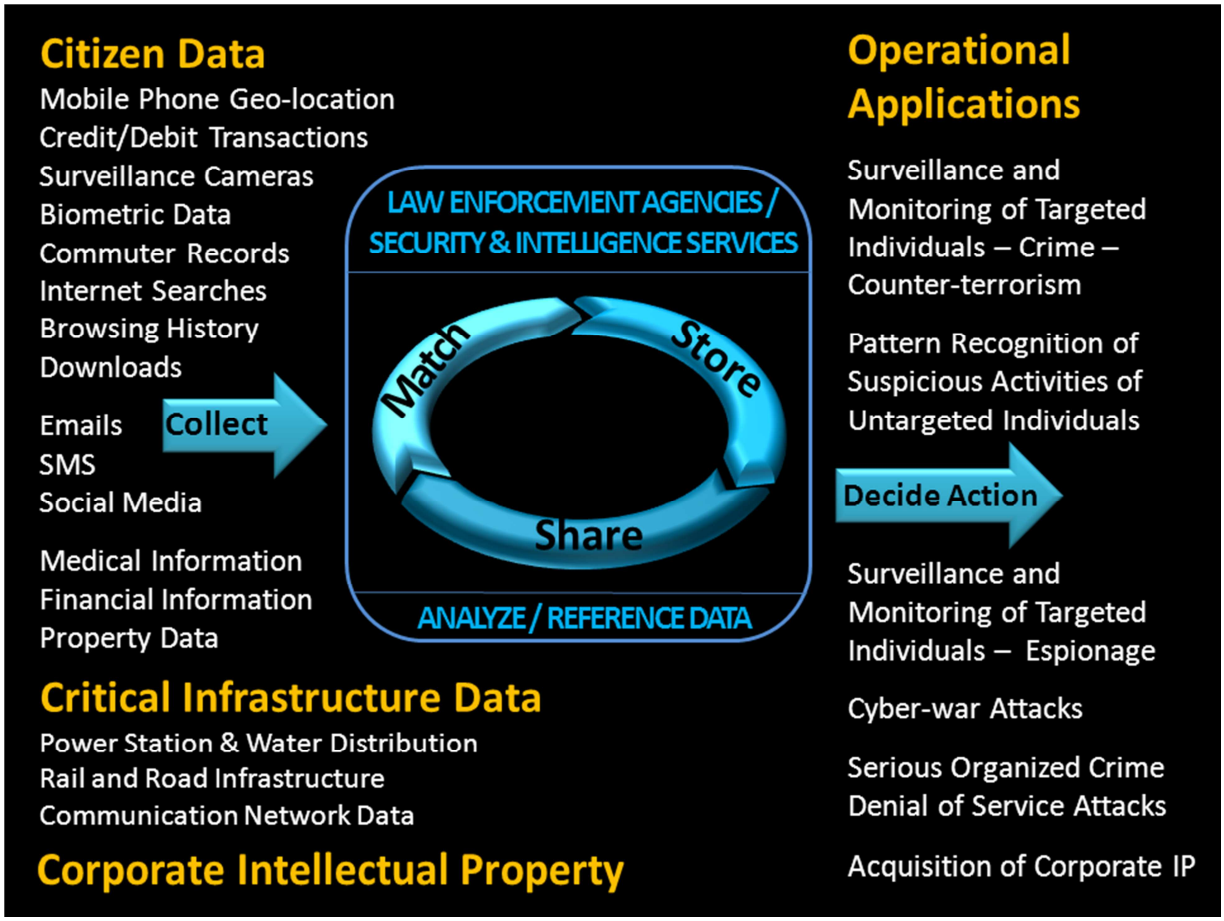
This “fitness for purpose” approach is perhaps especially important in the post-Snowden era where both the citizen and the policy maker are increasingly asking – and are being asked – legitimate questions such as “Does existing data protection law adequately regulate the situation to protect citizens from overly-intrusive surveillance of the type revealed by Edward Snowden”? and “If not, will the new laws being discussed at the European level adequately protect the citizen?” or “Is there any real difference in practice between the way the police and other law enforcement agencies (LEA) obtain and use personal data and the way this is obtained and used by security and intelligence agencies (SIS)?” “what degree of overlap may exist between LEAs and SIS in real life?”.

The Facts – as part of the benchmark for deciding whether new laws are “fit for purpose”

1. How data travels – zillions of packets all jumbled together down a fiber-optic “pipe”

The first pertinent fact here identified is one of the technical dimensions that policy makers will have to consider: the difficulties imposed by the way data flows over fiber-optic cables. These days relatively less data traffic is being carried via satellite while more and more data traffic is being carried across an ever-increasing number of fiber-optic cables snaking across continents and under the sea to other continents, While they may sincerely wish to avoid mass surveillance, politicians the world over must face the fact that a fiber-optic cable is a clean fresh water-mains and a sewage pipe all rolled into one. The data that flows through “the pipe” may contain a whole mixture of citizen’s private correspondence, e-commerce transactions, various forms of cybercrime including organized crime botnets, private and state-assisted industrial espionage, state-sponsored cyber-attacks etc. in such a way that the clean water is constantly mixed with the filth. The challenge that exists for police and intelligence services everywhere and anywhere is how to filter the clean water out and just leave the filth and then again depending on which filth they are looking for.

This first fact is hopefully better illustrated in the diagram below. Three categories of data appear on the left-hand side of the diagram: personal data identified as “Citizen data” and non-personal data identified as “Critical Infrastructure Data” and “Corporate Intellectual Property”. These flow together over the same fiber-optic cable which can be tapped for the data flow to be analyzed by the LEAs and/or the SIS. This analysis is carried out using a number of so-called “selectors” which then help monitor targeted individuals known to be criminals or terrorist suspects or else to seek out patterns of behaviour which may be suspicious or reveal new trends and links in criminal or terrorist behavior. Down the same pipe a commercial espionage and/or denial of service attack may be carried out on a large scale on commercial companies and/or critical infrastructure. These type of cyber-attacks may also be carried out on behalf of serious organized crime by sophisticated cyber-criminals creating and hiring out botnets, or else be state-sponsored probes or outright state-sponsored attacks on a foreign target. They all go down the same “pipe” and, in order to obtain actionable intelligence, to mix metaphors, the wheat must be sorted from the chaff.



It should be noted that the category of "Citizen data" may itself be sub-divided into several other important categories of which four are here summarily described. The first of these categories is that which in the RESPECT project has been termed as "Non-Surveillance data"[4] and which consists of data which was generated by a citizen's transactions and which was not originally ever intended to be used for surveillance purposes. This includes data like mobile phone records originally generated to permit mobile calls to be routed or billed but which also permit the user of that phone to be located with a fair degree of accuracy at a given moment in time in a specific geographical place. Likewise the electronic trails left by credit or debit card transactions in stores around town or on the internet. Using one's mobile phone or one's credit card to pay when one is "off-line" out on a shopping trip to the mall creates electronic foot-prints that travel and can be accessed on-line. The same individual's activities on-line, his or her internet searches, browsing history, down-loads and on-line purchases are also being stored, processed and sometimes onward communicated by several for-profit corporations in the private sector. As are a second important sub-category, the citizen's communications in the form of e-mail, SMS texts and VOIP telephony. Unlike the first sub-category this is actually content-data, very often the type of correspondence to which several national constitutions around the world have ascribed a right to privacy and confidentiality. A common denominator between all this data which can

[4] See definitions in Deliverable D2.1 of the RESPECT project available at www.respectproject.eu

reveal so much about an individual is the fact that most of it is collected and stored by for-profit corporations in the private sector.

A third sub-category is that of social media data, information about oneself which the user may have intentionally put on-line sometimes for everybody to access but increasingly often only intended to be shared with a circle of friends and acquaintances. The fourth sub-category of personal data is that of information given voluntarily by the individual for a specific purpose such as medical information, financial information or property information.

All of the above four sub-categories of personal data form part of a torrent consisting of petabytes of all possible types of data travelling down a fiber-optic cable literally at the speed of light. The same cable will carry attacks carried out by botnets on private companies or state institutions, industrial espionage attacks on corporations, or even cyber-war type attacks intended to disable power stations, water utilities or road, rail or communications networks. Knowing which string of bytes, which "packet" is which, is what LEAs and/or more often SIS try to determine, ostensibly in an effort to detect and prevent or prosecute crime or terrorism. Intercepting and analyzing the signals going down several fiber-optic cables lies at the heart of, for example, the TEMPORA programme carried out by GCHQ in the UK[5]. The Snowden revelations[6] have confirmed another dimension of this first fact i.e. that interception of personal data is both rife and indiscriminate – and, given the way that all sorts of data travel down a fiber-optic "pipe", at its start point, the interceptions cannot be anything but indiscriminate with unwanted data being later discarded at some point during the analysis process.

2. The impact of changing business models, consumer behavior and digitisation

The result of 20-25 years of "going digital", of changing business models and the advent of the internet has meant that vast quantities of personal data which were previously unrecorded or inexistent are now being collected and analyzed. Before the advent of the Internet and the World Wide Web it was, by definition, not possible to generate data about internet searches, downloads or browsing history. Nor was it a fundamental part of the business model of corporations like Google or Facebook to profile their customers in order to attract revenue generated by targeted advertising. Until just over twenty years ago most people did not carry mobile phones and thus did not generate an entirely new class of transactional and geo-location data about themselves. As a result, whereas until 25 years ago the main concern of the privacy-conscious citizen may have been the collection and use of data about him or her by the state, in reality today the collection of personal data by the private sector far outstrips that of the state. LEAs and SIS are very keen to access that personal data held by the private sector and sometimes are accorded legal forms of coercion by the law in order to obtain that data from private-sector

[5] See multiple articles about these activities available at www.guardian.com , www.derspiegel.com etc.
[6] ibid

corporations. It is the frequency and transparency as well as the necessity of that entire access process which the Snowden affair has increasingly brought into focus.

3. The use of the Internet for industrial espionage

Although most recently highlighted by the Alcatel-Lucent case,[7] there have been many cases where industrial espionage on the Internet has attracted international attention. It would also appear that some of this is state-sponsored while the precise extent of the problem is hard to gauge.

4. The need for harmonization of European and indeed international law

The changing business models highlighted in the second pertinent fact outlined above means that especially in the case of large multinational corporations but also with the operations of many SMEs, personal data is now being held across many jurisdictions with serious consequences for effective legal regulation. As Angela Merkel put it when speaking about the situation in Germany "We have a great data protection law. But if Facebook is registered in Ireland, then Irish law is valid, and therefore we need unified European rules"[8]. German frustration at such a situation may have been especially increased by a decision of a German court in May 2013 that it was Irish Law and not German law that was applicable to Facebook, thus avoiding the enforcement of German regulations in German territory.[9]

5. Reliance of LEAs and SIS on personal data held by the private sector

Which brings this analysis to a fifth fact: Police and state security services are much more reliant on data held by the private sector than at any time in the past or more than they ever thought they would be. While this may be greatly cost-efficient at times where severe economic constraints are placed upon LEAs, it brings into sharp focus the conditions under which LEAs and SIS may expect to have access to that data as well as those instances in which those corporations may process and onwards-sell the results of their analysis of personal data.

[7] "NSA Busted Conducting Industrial Espionage In France, Mexico, Brazil, China and All Around the World" washington's blog last accessed on 29 october 2013 at http://www.washingtonsblog.com/2013/10/nsa-busted-conducting-industrial-espionage-in-france-mexico-brazil-and-other-countries.html

[8] BBC New Europe "German Chancellor Merkel urges better data protection rules" 14 July 2013 last accessed on 20 October 2013 at http://www.bbc.co.uk/news/world-europe-23309624

[9] Piltz Carlo, "Facebook subject to Irish, not German, data protection law, says German Higher Administrative Court" 23 May 2013 last accessed on 20th October 2013 at http://blogs.olswang.com/datonomy/2013/05/23/facebook-subject-to-irish-not-german-data-protection-law-says-german-higher-administrative-court/

6. Public sentiment: People care about privacy – well, some people to some extent

This sixth fact is not as universal as one would have thought and a number of writers have questioned whether apathy[10] or ignorance affect the extent to which people feel strongly about privacy. There is growing evidence to suggest that Europeans do care about privacy, that their awareness of being monitored should not be construed as or be confused with their acceptance of being watched[11] and that many people object to large-scale integration of personal data about them.[12] Other data also suggest that people in the USA are torn between their concern about security and their wish for privacy[13]. Germans have been amongst those most given to public demonstrations in favour of privacy[14] yet pre-poll data in the 2013 German elections suggested that security and privacy came bottom of a list of concerns presented to the German electorate[15]. While the next sets of empirical data from projects such as RESPECT[16] are eagerly awaited, it should be said however that there is little or no evidence to suggest that Europeans or indeed Americans feel very differently if they realise that they are being spied upon by the police, by a secret service or by a private company. While some evidence suggests that some people trust the state more with their data – or vice-versa- what people don't like is being spied upon irrespective of who carries out the spying.

7. The harmonization of Data Protection law in the police sector is not a novelty-it has come of age

A seventh fact pertinent to a discussion about the data protection law in the sector, is that there exists a fair amount of legislation in Europe which is intended to regulate the use of personal data by the police and other LEAs. This type of legislation has, most recently, been extensively surveyed in 31 member states of the Council of Europe by the PUPIE project[17] which clearly demonstrates that the harmonization of laws of many European states has been a Work-in-progress since the Council of Europe launched its Recommendation R(87)15 over twenty-five years ago. The extent to which

[10] See for example John Naughton " Edward Snowden: public indifference is the real enemy in the NSA affair Most people don't seem to worry that government agencies are collecting their personal data. Is it ignorance or apathy?" The Observer, Sunday 20 October 2013 last accessed on 29th October 2013 at http://www.theguardian.com/world/2013/oct/20/public-indifference-nsa-snowden-affair

[11] See various results of empirical quantitative and qualitative research with on-line users from the CONSENT project as progressively published at http://www.consent.law.muni.cz/

[12] See results of empirical qualitative research about citizen perceptions of surveillance from the SMART project as progressively published at http://www.smartsurveillance.eu/

[13] JENNIFER AGIESTA; DIGITS: Torn between civil liberties, terrorism— Sep. 17, 2013 12:30 PM EDT The Big Story Associated Press last accessed on 29th October 2013 at http://bigstory.ap.org/article/digits-ambivalence-civil-liberties-terrorism

[14] See reports on demonstrations at http://bigstory.ap.org/article/protest-rally-suspected-german-nsa-site and http://rt.com/news/germany-nsa-merkel-writers-669/

[15] The most recent voter survey conducted by public broadcaster ARD saw intelligence agencies' surveillance ranked last among six other campaign topics that included tax policy, pensions and pay and work conditions. Just 17 percent described the issue as relevant. As cited in Opposition banks on NSA in German elections" Deutche Welle 10 Sep 2013 last accessed on 20 October 2013 at http://www.dw.de/opposition-banks-on-nsa-in-german-elections/a-17076974

[16] See http://respectproject.eu/

[17] "Recommendation R (87) 15 – Twenty–five years down the line" Report by Professor Joseph A. Cannataci and Dr. Mireille M. Caruana first submitted on 12 November 2011 with a revised version eventually later submitted on 26 September 2013 for consideration by the Council of Europe's Consultative Committee on Data Protection T-PD; Since completed with data from 31 European states and presented in person to the T-PD Plenary session on 15th October 2013. Officially restricted and due to be formally published on-line by the Council of Europe after final corrections and proof-reading before end December 2013, this report was leaked to Statewatch by unknown persons in September 2013 following its being made available to T-PD members. That 26 September 2013 version is available at http://www.statewatch.org/news/ and specifically downloadable at http://www.statewatch.org/news/2013/oct/coe-report-data-privacy-in-the-police-sector.pdf

European law in the sector has been harmonized, especially since R(87)15 became the data protection standard for the Schengen area in 1989 and part of the *acquis communitaire* of the European Union has been discussed in previous publications between 2006 and 2010[18]. The 2010-2013 research presented in the results of the PUPIE project are but the most recent confirmation that harmonization of European law in the police and criminal justice sector has been an on-going process for the best part of a quarter of a century. The PUPIE report confirms that there remain a number of areas which may still benefit from an increase in clarity and further harmonization between the legal provisions existing in member states of the Council of Europe – of which the EU is an important sub-set - but it certainly is not virgin territory for the legislator.

8. Existing laws intended to regulate police use of personal data were designed to tackle an old reality and not the new one

The conclusion reached by the authors of the PUPIE report reflects the fact that much of the current European legislation was designed to afford citizens protection of their data which had been collected by an LEA "for police purposes". As indicated above, today much of the data that is accessed by LEAs and SIS has been collected by the private sector for purposes which are not "police purposes" as defined by the leading European legal instrument in the field Rec(87)15[19]. This leads to a debate as to whether LEA and SIS purposes are compatible purposes for onward processing of personal data collected for purposes as diverse as credit card or mobile phone bill payment or leisure or work on-line behaviour. A debate which as will be seen later hinges on the notions of "necessity" and "proportionality". Moreover there is a huge disparity in the type of legislation and oversight that exists within European states to regulate the activities of SIS as distinct from LEAs, something which is also remarked upon in some detail in the PUPIE report[20]. This has led to a situation where it cannot be accurately said that the use of personal data by LEAs or SIS is not regulated. In many cases it is regulated. The point remains however "Is it adequately regulated?" Is the privacy of the citizen afforded adequate protection from overly-intrusive surveillance by LEAs and SIS? The Snowden revelations suggest that the levels of interception and analysis are enormous and that the levels of protection and oversight are inadequate. So much so

[18] Joseph A. Cannataci, Study on Recommendation No. R (87) 15 of 17 September 1987 regulating the use of personal data in the police sector "Data Protection Vision 2020 Options for improving European policy and legislation during 2010-2020" Strasbourg, 4 November 2010 T-PD-BUR(2010)12 FINAL;
J. A. Cannataci (2010) Squaring the circle of smart surveillance and privacy, Fourth International Conference on Digital Society, ISBN 978-0-7695-3953-9/10 DOI 10.1109/ICDS.2010.55, 323-328
J.A. Cannataci & J. P. Mifsud Bonnici, (2010) The end of the purpose-specification principle in data protection? International Review of Law, Computers and Technology, Routledge, UK ISSN: 1364-6885 (electronic) 1360-0869 (paper) Vol. 24, No.1, March 2010 pp 1-17, DOI: 10.1080/13600861003637693
Joseph A. Cannataci, Mireille M. Caruana and Jeanne Pia Mifsud Bonnici, (2006) 'R (87) 15: A slow death?' in "Monitoring and Supervision" Erasmus University Press, Rotterdam., pp. 27-49, ISBN 905677316X

[19] See introductory section "Scope and Definitions" of RECOMMENDATION No. R (87) 15 OF THE COMMITTEE OF MINISTERS TO MEMBER STATES REGULATING THE USE OF PERSONAL DATA IN THE POLICE SECTOR (Adopted by the Committee of Ministers on 17 September 1987 at the 410th meeting of the Ministers' Deputies) which stipulates "The expression "for police purposes" covers all the tasks which the police authorities must perform for the prevention and suppression of criminal offences and the maintenance of public order."

[20] "Recommendation R (87) 15 – Twenty–five years down the line" Report by Professor Joseph A. Cannataci and Dr. Mireille M. Caruana first submitted on 12 November 2011 with a revised version eventually later submitted on 26 September 2013 for consideration by the Council of Europe's Consultative Committee on Data Protection T-PD *op.cit. supra*.

that inquiries and investigations have commenced or revelations made in the UK[21], France[22], Germany[23], the USA as well as by the EU[24] and separately the Article 29 Working Party[25]. Snowden-style interceptions and analysis seem to be the new reality whereas existing laws appear to have been designed to deal with a different older reality and, certainly for those laws inspired by Rec(87)15, namely the data collected by the police for their own purposes and not interception of or other access to data collected by the private sector as indicated in various instances above.

9. LEAs and SIS collaborate to a considerable extent in many European and non-European states

In many states SIS do not have executive powers, although there do exist a few exceptions especially in the case of anti-terrorist activities. In most cases however the prime function of the SIS is to produce "actionable intelligence" which is then passed on to the LEAs to take action about whether it is to further monitor, follow, detain, arrest or prosecute a person or group of persons. This fact about the practices of LEAs and SIS raises two important considerations especially in the light of the Snowden revelations: a) does it make sense to have a strict data protection regime covering the collection and use of personal data by the police and then have a much "lighter-touch" regime for the SIS if the SIS are then going to give the results of their findings to the police? In other words if the regulatory regimes for LEAs and SIS are out of synch then a route for circumvention of data protection law principles may exist; b) the degree of collaboration between SIS located in the USA, UK and Australia to name but three countries is such as to have raised serious doubts as to the extent to which these agencies do not accord themselves a domestic remit although they are primarily supposed to be focusing on foreign citizens. There have been allegations that "scratch my back and I'll scratch your's" arrangements such that data about US citizens that could not be legitimately collected by the USA was collected on its behalf by GCHQ in the UK and vice-versa. If these allegations turn out to be true then this is yet another form of circumvention of legal rules intended to ensure that the prying eyes of the SIS were used only for "suspicious people and normally foreigners" rather than nationals.

[21] Nick Hopkins, Patrick Wintour, Rowena Mason and Matthew Taylor, "Extent of spy agencies' surveillance to be investigated by parliamentary body Intelligence inquiry begun after Edward Snowden leaks and Guardian revelations on GCHQ and NSA personal data sharing, The Guardian 17 October 2013 Last accessed on 29th October 2013 at http://www.theguardian.com/uk-news/2013/oct/17/uk-gchq-nsa-surveillance-inquiry-snowden

[22] Per lijas U.S. Ambassador to France Summoned Over New Snowden Leaks TIME 21 October 2013 last accessed on 29 October 2013 at http://world.time.com/2013/10/21/u-s-ambassador-to-france-summoned-over-new-snowden-leaks/#ixzz2jHodXzpI

[23] Veit Medick and Annett Meiritz "NSA Scandal: Parliamentary Spying Inquiry Poses Challenges" last accessed on 29 October 2013 at http://www.spiegel.de/international/world/germany-faces-challenges-in-investigating-nsa-spying-a-930639.html
Derek Scally and Guy Hedgecoe , German parliamentary inquiry into scope of US spying may call Snowden, The Irish times, last accessed on 29th October 2013 at http://www.irishtimes.com/news/world/europe/german-parliamentary-inquiry-into-scope-of-us-spying-may-call-snowden-1.1576101?mode=print&ot=example.AjaxPageLayout.ot

[24] Civil Liberties delegation to Washington DC to probe US mass surveillance of EU citizens EU Parliament, last accessed on 29 October 2013 at http://www.europarl.europa.eu/news/en/news-room/content/20131024IPR23002/html/LIBE-delegation-to-Washington-DC-to-probe-US-mass-surveillance-of-EU-citizens

[25] Donald G Aplin EC Privacy Advisers Detail PRISM Probe, Question Viability of U.S.-EU Safe Harbor, Bloomberg BNA 19 August 2013 last accessed at http://www.bna.com/ec-privacy-advisers-n17179875930/

10. The importance of the Deep Web or the Undernet to Terrorism and Organised Crime –

As already pointed out in the Data Protection Concept report[26] it is suspected that the vast bulk of terrorist and serious crime activity on the Internet is not carried out in those parts of Cyberspace normally frequented by the vast majority of law-abiding citizens. Rather, as suggested in a report published by the Dutch Intelligence Agency, aspiring or actual terrorists such as Jihadis and/or criminals and/or organized crime syndicates dealing with drugs, paedophilia etc. inhabit that part of cyberspace known as the Deep Web or the Undernet. If this fact is further proven, then two considerations need to be highlighted: firstly that LEAs and SIS would be looking for leads in the wrong place if they were to focus indiscriminately on the on-line and off-line electronic tracks left by the vast majority of the population; secondly that further intense international collaboration may be required to properly infiltrate and where appropriate occupy the Deep Web and identify the criminals and terrorists operating there.

11. As more and more data is produced, more and more automated analysis of the data is required

The quantity of data which is being generated and which may need to be analysed is increasing exponentially and has in many cases already reached levels where human analysis of that data in the first instance is impossible. LEAs and SIS simply do not have the levels of staffing required to manually sift through the petabytes of data created and circulating on a daily basis. The proportion of human analysts to data quantities is set to shrink further over the coming years. It is therefore a fact that more and more automated analysis of data is to be expected over the coming years. The creation of the software used for such analysis and the audit trails and choice of "selectors" utilized by such software will doubtless become part of the focus of data protection regulators and practitioners as they try to strike the right balance between security and privacy. It is perfectly conceivable to create and maintain intercept programmes where, for example, automated voice-recognition and face-recognition technologies would be applied to data flows. There could be perfectly legitimate reasons for carrying out such automated analysis provided that the right legal basis and a host of legal, technical and operational safeguards are in place. As demonstrated by the PUPIE project[27] however none of the member states of the EU or the European Union have yet identified a set of safeguards and legislated

[26] Cannataci, Joseph A. 2013. Concept paper on the application of data protection regulations in relation to transborder private/public information sharing for (a) network security purposes and (b) criminal justice purposes. Concept paper commissioned by the Council of Europe produced in two versions December 2012 and September 2013, published by the Council of Europe on 07 November 2013.pp.28-29 at http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/Octopus2013/2467_intern_information_sharing_JACannataci_v5.pdf

[27] "In general, States do not appear to have attained practical implementation of the related principle laid down in Art.7, CFD 2008/977/JHA dealing with "automated individual decisions", equivalent to Art.9, proposed Police and Criminal Justice Data Protection Directive which refers to "measures which produce an adverse legal effect for the data subject or significantly affect them and which are based solely on automated processing of personal data intended to evaluate certain personal aspects relating to the data subject". The responses (or lack of them) to the questionnaire suggest many EU States are unprepared for implementation of either Art.7, CFD 2008/977/JHA or Art.9 of the draft Directive which both require specific laws with appropriate safeguards." PUPIE Project Report Page 16.

them into being, despite the fact that they are required to do so by both Rec(87)15[28] and the EU's Council Framework Decision CFD/977/JHA of 2008.

12. A more international approach to dealing with crime and terrorism

As crime and especially serious organised crime becomes more global there is a real need to seek and create co-ordinated international responses to detect, prevent and/or prosecute such criminal activity. The international collaboration required to provide a timely response to various forms of threats may of course be limited to exchange of information through traditional bilateral methods or through contributing to and accessing databases such as those held by INTERPOL and EUROPOL. As seen above, the quantity of data which needs to be analysed is however increasing exponentially to levels where even the exchange of data across borders may need to be automated. LEAs and SIS are notoriously reluctant to pass information to anybody except very trusted partners yet it is not inconceivable that slowly but surely a number of LEAs and SIS will collaborate together to the extent that they may enable fast and even automated access to certain types of personal data, especially in those instances where it is felt that rapid, sometimes instantaneous access could help prevent real dangers or serious crimes. If properly done in the right context it is equally conceivable that such exchange of data would be done in full respect of the letter and the spirit of data protection law. The building of trust and mutually accessible sub-systems is a process which takes years to create but, as the Five Eyes example has demonstrated, not impossible to achieve. Moreover, internationally accessible databases such as those operated by INTERPOL and EUROPOL, all subject to high levels of personal data protection, are expected to see continuous growth in both content and use with an increasing use of biometrics as well as voice-recognition, face-recognition and gait recognition capabilities. Although, in the context of the Draft Directive, both the UK Government[29] and the Bundesrat[30] have claimed that the case for harmonization of criminal justice procedures has not yet been properly made, in effect the ground rules for analogous ground rules in the sector have already been agreed in the context of the Cybercrime Convention[31]. There the concern about the need for the detection, prevention and prosecution of crime in cyberspace and the concomitant needs to obtain and preserve evidence have led to a consensus broad enough to

[28] The responses to this question suggest that there is no common understanding of the term "technical surveillance or other automated means" among the States surveyed; national laws are not harmonized; and/or police practices, in so far as technical or other automated means of surveillance is concerned, vary from State to State. (PUPIE Report op.cit. Page 16)

[29] in its 895th session on 30th March 2012, the Bundesrat adopted Decision 51/12 Decision pursuant to Article 12, Point b, TEU:30 March 2012 last accessed on 29 October 2013 at http://www.google.com.mt/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&ved=0CC8QFjAA&url=http%3A%2F%2Fwww.ipex.eu%2IPEXL-WEB%2Fdossier%2Ffiles%2Fdownload%2F082dbcc53782a3ff01378425d0850186.do&ei=1pJwUuvWEIKVtQann4DoAQ&usg=AFQjCNFcQGoMvpA165PDcpnwMPM4E1FtWg

[30] Justice Select Committee's opinion on the European Union Data Protection framework proposals Presented to Parliament by the Lord Chancellor and Secretary of State for Justice by Command of Her Majesty, January 2013 last accessed on 29 October 2013 at http://www.parliament.uk/business/committees/committees-a-z/commons-select/justice-committee/inquiries/parliament-2010/eu-data-protection/

[31] Convention on Cybercrime, Budapest, 23.XI.2001, European Treaty Series 185 last accessed on 29th October 2013 at http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

attract a number of countries including the United States to join the vast majority of leading European states in agreeing to a number of applicable rules. As the proportion of on-line crime grows when compared to the more traditional off-line variety, so does the awareness grow that all sorts of criminals, whether carrying out criminal actions on-line or off-line, also have an on-line presence or may leave electronic tracks which may be followed in the on-line environment. When coupled with the needs to harmonize the collection and transmission of electronic evidence across and beyond Europe the arguments for further harmonization of the sector continue to stack up.

13. THE EU has no competence in matters of national security

There can be little doubt that the exclusion of competence of EU institutions and EU law in matters of national security in terms of Art 4 Section 2 of the EU Treaty would be successfully invoked by one or more EU Member States so matters dealing with national security such as intelligence and surveillance of the type revealed by Snowden are ultra vires to EU institutions[32].

14. The trans-atlantic context requiring good relations.

While public utterances in the wake of the Snowden affair, suggest that countries like Germany, France and Belgium are far more upset at the USA than, say, the UK, it should be assumed that the UK, Germany, France and several other countries do not wish to harm a sometimes useful collaboration with the US security agencies.

The Risks

The facts considered above suggest that a number of risks need to be managed. In summary, these include*:*

I. The way that data travels over fiber-optic cables means that LIS/LEAs very often require that mass interception and mass storage must take place to permit effective monitoring. This creates the risk of mass surveillance as well as an attractive target for hackers.
II. Using data for profiling enables companies to manipulate consumers – tell them only that which suits them – what they think they want to hear – conveniently leaving out those bits which they know consumers would not want to hear – the omission approach – otherwise known as being economical with the truth

[32] "The Union shall respect the equality of Member States before the Treaties as well as their national identities, inherent in their fundamental structures, political and constitutional, inclusive of regional and local self-government. It shall respect their essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security**. In particular, national security remains the sole responsibility of each Member State".** Emphasis added Art 4 Section 2, Consolidated version of the Treaty on European Union, Official Journal of the European Union

III. Using data obtained through profiling and from on-line surveillance, the state may target its internal opponents using illegitimate means
IV. The state may manipulate information in exactly the same way as private corporations in order to stay in power
V. The quality of automated analysis is only as good as the knowledge engineering and the programming behind the software concerned
VI. automated analysis may occasionally lead to adverse affects and wrong decisions

The significance of form – Regulation, Directive, Recommendation and Convention[33]

Much of the following discussion needs to be understood in context and since the analysis perforce moves to and fro a European context as well as within a broader international context it may be well worth pausing an instant to differentiate between certain forms of legal instruments which may be pertinent.

The German Parliament and the UK Parliament amongst others have for example delivered lengthy opinions as to whether for example the DPRP should take the form of a Directive and not a Regulation, while this study will very often refer to other forms of legal instruments such as a Recommendation or a Convention.

On the 25th January 2012 the European Commission published two, not one, proposals for new legislation in the ever-growing field of privacy and data protection. One of these two proposals is the mildly-named but potent "Regulation". As such this is the most direct form of EU law - as soon as it is passed, it will have binding legal force throughout every Member State. This new regulation takes the European omnibus approach to privacy to even higher levels. It covers most areas of data protection and is capable, in due course, of being applied to most walks of life: health data, insurance data, social security data and so on. The proposed regulation is one step up and different from a directive which is addressed to national authorities, which must then take action to make it part of national law. Indeed the Commission's main objection to the existing regime created by Directive 95/46/EC is precisely that it is governed by a directive and not a regulation thus leading to fragmentation and a lack of uniformity across 27 EU member states.

The debate about form is significant since, in terms of EU law, when viewed from the perspective of a national parliament within the EU, a Regulation is the most intrusive piece of legislation possible. There is no leeway for any EU member state when it comes to a Regulation: the very wording of the Regulation approved through due process by the European Parliament amd the Council of Ministers, becomes the law in the member state, thus producing an identical law in each of the 28 member states. A Directive, on the other hand, allows significantly more wriggle-room. A Directive lays down principles

[33] This paper was specifically written for publication in the European Journal of Law and Technology which is well known to have a wide international readership some of whom may not be familiar with the distinctions between certain European legal instruments. Readers who are confident that they do know the differences between the legal instruments in this caption can safely skip this section.

albeit sometimes at a considerable level of detail, which the individual state then has to transpose to its own national law. This leaves room for the member state's own interpretation of the Directive and while in theory this allows for implementation of a principle in different cultural, social and economic contexts, in practice it also often may lead to a result of "lost in translation" and 28 different legal regimes. In the context of data protection law and large multinational firms this has been alleged to be an important factor and cost-element insofar that a business wishing to operate across Europe is faced with not one but 28 different legal regimes to comply with. This may add compliance costs to the business which in turn makes that business less competitive and its products or services more costly to its European and other customers. This is precisely why of one the business-friendly aspects of the DPRP is that it will introduce a "one-stop shop" provision such that the business operator will have to comply only with the law of the chosen principal place of business in the EU.

National Governments within the EU often resist proposed Regulations because they are more internally disruptive than Directives. In other words if, say, the German courts or the British courts have been accustomed to doing things in a certain way for decades or centuries and a new draft European law would direct them to do things differently, there is bound to be a lot of himming, humming and hawing as to whether this is a good idea or not and the more conservative elements within those legal systems will often make attempts to pay lip-service to the new European law while retaining "the good old way of doing things" intact.[34] In such instances it has become a reflex action to try to get the new European law formulated as a Directive instead of a Regulation. There may of course sometimes be perfectly good and valid reasons for choosing a Directive as the legislative vehicle rather than a Regulation yet there is no doubt that some EU member states "play the system" and often try to water down proposed changes by opting for a Directive instead of a Regulation.

Non-Europeans sometimes may not realize that one must be very careful when one speaks of "European Law". Confusingly enough for both Europeans and non-Europeans there is not one Europe but two and there are at least two bodies of European Law. Directives and Regulations are legal instruments of European Union Law[35] and the European Union consists of 28 countries and just over 500 million inhabitants. Yet, those 28 countries are not only members of the EU but also hold dual membership. They form part of the wider – and older – European family which is called The Council of Europe (CoE) which groups 47 member states and 820 million inhabitants. Thus, by way of example, Romania is a member of both the EU and the CoE but Russia is only a member of the CoE. The latter has long established itself as the most prominent international body responsible for Human Rights Law. The European Law emanating from the Council of Europe arrives through legal instruments which are different to the Regulation and Directive mentioned above. The CoE depends on binding multilateral treaties which are called "Conventions" which operate very much like Directives within the EU. A CoE Convention sets out goals but it is up to member states to decide how in their own law those goals will

[34] The author's experience of over 25 years of participating in the negotiation of different legal instruments has seen countless hours of bickering between the representatives or nominees of different countries, all trying to ensure that the new proposals on the table require the least possible change, if any, back home. That change and positive change does happen is testament to the strength of the idea as much as its proponent.

[35] For a concise differentiation of different legal instruments under EU law see http://europa.eu/eu-law/decision-making/legal-acts/index_en.htm

be achieved. The EU's current Data Protection Directive dating from 1995 is in fact very largely inspired by and modeled upon the CoE's Convention 108[36] CoE Conventions are also terrifically useful instruments from the international law perspective since they are very often open for signature to non-European countries. Thus, if a European idea is really good it can be exported easily to those countries which sign up to it. Classic examples include Australia, Japan and the USA[37] adhering to the Cybercrime Convention[38] and Uruguay ratifying the Data Protection Convention.[39]

This study will also make extensive reference to another form of legal instrument, the Recommendation which, again confusingly, is used as a term by both the EU and the CoE and which, in essence, is a non-binding form of law which however may be very influential. This is sometimes called "soft law"[40] In the field of data protection in the police sector the major source of European law to date has actually been a piece of "soft law" ie Recommendation R(87)15 the impact of which has been examined in detail elsewhere. [41] These distinctions are especially important and pertinent to this present study since, as will be seen later, policy-makers in the EU have an important option to exercise: in those cases where the rules of the EU do not permit certain forms of law to be made within and by EU institutions, it is possible to have the same legal principles transformed into law by going through the Council of Europe. This is, as will be seen, particularly important for a discussion on "surveilling surveillance" in the post-Snowden era where one of the main forms of justification for surveillance is national security, an area of activity and law which is precluded from EU jurisdiction and is a competence reserved to member states.[42] Those same member states however may choose to bind themselves in matters concerning surveillance and national security through an international treaty such as a convention negotiated within and promoted by the Council of Europe, an avenue for action explored in the concluding sections of this paper.

[36] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data Strasbourg, 28.I.1981 last accessed on 29th October 2013 at http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm and http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CL=ENG

[37] Signatories to the Convention on Cybercrime, Budapest, 23.XI.2001, European Treaty Series 185 last accessed on 29th October 2013 at http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CL=ENG

[38] Convention on Cybercrime, Budapest, 23.XI.2001, European Treaty Series 185 last accessed on 29th October 2013 at http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

[39] Signatories to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data Strasbourg, 28.I.1981 last accessed on 29th October 2013 at http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CL=ENG

[40] The extent to which Recommendation R(87)15 is influential and can be termed as soft law is reflected upon at Cannataci, Joseph A. 2013. Concept paper on the application of data protection regulations in relation to transborder private/public information sharing for (a) network security purposes and (b) criminal justice purposes. Unpublished paper commissioned by the Council of Europe produced in two versions December 2012 and September 2013, due to be published by the Council of Europe before 06 December 2013.pp35-37

[41] See discussion of Fact 7 in the main text of this paper as well as the publications indicated in footnotes 17 and 18 earlier.

[42] Art 4 Section 2, Consolidated version of the Treaty on European Union, Official Journal of the European Union C326 26 October 2012 See full text in footnote 32 supra..

The significance of data exchange – why is the law important and useful?

A proposal to have a new law such as the draft Directive[43] may be very important for a number of practical reasons:

1. Both existing and proposed European data protection laws lay down restrictions on the export of personal data from member states but generally permit the transfer of such data within the "European Data Protection Club". The key idea here is that non-sensitive personal data may circulate freely within and between those countries which have agreed to respect the common European values entrenched in the data protection law principles while special conditions may be imposed for those countries which are not EU members or have not ratified and implemented the CoE's Convention 108.
2. LEAs and SIS in European and non-European states exchange personal data on a bilateral basis and by contributing to international databases such as those held by INTERPOL and EUROPOL. This process is important since currently in most cases there is a human intervention i.e. a human being inside an LEA or an SIS takes a conscious decision as to whether such personal data may be exported – and presumably safely exported - to another country or to an international database. In those cases the LEA or SIS official is expected to comply with the data protection law of his or her country which may or may not impose special restrictions on the processing and export of such personal data;
3. The huge growth in the volume of personal data capable of analysis is leading to more and more forms of automated analysis some of which may in turn lead to the automated population of suspect lists and wanted lists and other tools utilized by LEAs and SIS. An exponential growth is expected in this sector with the volume of personal data analyzed far outstripping the number of human beings available within LEAs and SIS to analyse such data. It is not inconceivable, indeed it is expected that, in the fullness of time, the results of such analysis will cross borders in a number of ways either by LEAs granting each other access to certain parts of their data repositories or through automated population of internationally shared databases. Whatever the form that this automated exchange of personal data may take its facilitation would often offer the advantage of instantaneous and timely exchange of LEA/SIS data at the international level which could be useful, sometimes critical, for the prevention, detection and prosecution of crime. The compliance with the local data protection law can likewise be automated. It is likewise expected that the structure of these ICT systems would be predicated upon a privacy-by-design/privacy-by-default approach which would assume that the laws are set up in such a way that the state to which personal data is being exported, whether manually or in an automated pre-determined fashion, offers at minimum an equivalent or superior level of protection than the state from which it is exported.
4. The mobility of citizens across borders is especially sacrosanct within the EU internal market with the result that any infractions of national or EU law may need to be pursued across borders

[43] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data /* COM/2012/010 final - 2012/0010 (COD) */

and evidence may also need to be transmitted and used across borders. To date every single European state retains its own judicial procedures which, for historical reasons, may vary widely from state to state. The problems inherent to the current unharmonized structure have not yet come to the fore since it is only a small minority of EU citizens which have needed to have recourse to multiple different procedures inside multiple EU or CoE member states. The problems created by different procedural laws and especially the different laws of evidence in different European states may often cause long delays and inconvenience. Harmonising the procedures for collecting, storing, using and transmitting evidence to common agreed standards may therefore hold considerable benefits not only within Europe but also internationally but it is expected that since this would inevitably mean change for everybody within those legal systems there will be much resistance and delay along the way.

In the case of the DPRP all of the above practicalities can come into play and have been the subject of comment and analysis at various levels.[44]

Inherent contradictions ab initio – defying the logic

The formal public utterances by the European Commission about the DPRP as published on the 25th January 2013 contained a number of inherent contradictions. First the citizen is led to believe that "A single law will do away with the current fragmentation and costly administrative burdens, leading to savings for businesses of around €2.3 billion a year. The initiative will help reinforce consumer confidence in online services, providing a much needed boost to growth, jobs and innovation in Europe."[45] This emphasis on "a single unified approach" is premised on the assertion that "In Europe, legislation on data protection has been in place since 1995. The Data Protection Directive guarantees an effective protection of the fundamental right to data protection. But differences in the way that each Member State implements the law have led to inconsistencies, which create complexity, legal uncertainty and administrative costs. This affects the trust and confidence of individuals and the competitiveness of the EU economy."[46]

[44] See for example a German analysis whereupon in its 895th session on 30th March 2012, the Bundesrat adopted Decision 51/12 Decision pursuant to Article 12, Point b, TEU:30 March 2012 last accessed on 29 October 2013 at http://www.google.com.mt/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&ved=0CC8QFjAA&url=http%3A%2F%2Fwww.ipex.eu%2FIPEXL-WEB%2Fdossier%2Ffiles%2Fdownload%2F082dbcc53782a3ff01378425d0850186.do&ei=1pJwUuvWEIKVtQann4DoAQ&usg=AFQjCNFcQGoMvpA165PDcpnwMPM4E1FtWg
As well as the UK analysis such as Justice Select Committee's opinion on the European Union Data Protection framework proposals Presented to Parliament by the Lord Chancellor and Secretary of State for Justice by Command of Her Majesty, January 2013 last accessed on 29 October 2013 at http://www.parliament.uk/business/committees/committees-a-z/commons-select/justice-committee/inquiries/parliament-2010/eu-data-protection/

[45] EU Press release 25 January 2012 last accessed on 29th October 2013 http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm

[46] Why we need to reform the EU data protection rules? Data Protection reform. Frequently Asked Questions, MEMO/12/41 Brussels, 25 January 2012 Last accessed on 29th October 2013 at http://europa.eu/rapid/press-release_MEMO-12-41_en.htm

The emphasis on an integrated approach continues in an explicit manner. In answer to the question "What will be the key changes? One finds the answer "A single set of rules on data protection, valid across the EU." [47] Now that last sentence is, in terms of EU law, very close to the definition of a Regulation, an impression that is reinforced by announcements that "the European Commission is now proposing a strong and consistent legislative framework across Union policies, enhancing individuals' rights, the Single Market dimension of data protection and cutting red tape for businesses"[48]

Then suddenly the emphasis on "A single set of rules on data protection, valid across the EU." disappears and instead one finds an explanation of the DPRP which no longer looks or feels like a single set: what the DPRP consists of is A Regulation (replacing Directive 95/46/EC) setting out a general EU framework for data protection and a Directive (replacing Framework Decision 2008/977/JHA16) setting out rules on the protection of personal data processed for the purposes of prevention, detection, investigation or prosecution of criminal offences and related judicial activities.

The logic is at times impeccable and sometimes impossible to follow. In one breath the Commission attempts to explain (quite plausibly) why a Directive would not be fit for purpose and why therefore a Regulation is needed ""Under Directive 95/46/EC – the EU's main legislative act in the field of data protection today – the ways in which individuals are able to exercise their right to data protection are not sufficiently harmonised across Member States. Nor are the powers of the national authorities responsible for data protection harmonised enough to ensure consistent and effective application of the rules. This means that actually exercising such rights is more difficult in some Member States than in others, particularly online."[49] Having made the point somewhat effectively, on page 10 of the same Communication one reads why, in the police and criminal justice sector, Europe has to move forward from CFD/977/JHA but not why the Commission is recommending that we move forward in that sector using a Directive and not a Regulation. The omission of an explanation makes one wonder if one is being told the whole truth. Elsewhere in the Communication by the Commission one reads more argumentation implicitly advocating the suitability of a Regulation and not a Directive: "Despite the current Directive's objective to ensure an equivalent level of data protection within the EU, there is still considerable divergence in the rules across Member States. As a consequence, data controllers may have to deal with 27 different national laws and requirements. The result is a fragmented legal environment which has created legal uncertainty and uneven protection for individuals."[50]

Having thus attempted to convince the reader of the desirability of a Regulation over a Directive, the consequences in terms of logic should be obvious. Since, as the Commission is advocating, a Directive is

[47] How will they help businesses? Data Protection reform. Frequently Asked Questions, MEMO/12/41 Brussels, 25 January 2012 Last accessed on 29th October 2013 at http://europa.eu/rapid/press-release_MEMO-12-41_en.htm

[48] Ibid.

[49] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Safeguarding Privacy in a Connected World A European Data Protection Framework for the 21st Century/* COM/2012/09 final */25 January 2012 last accessed on 29th October 2013 at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52012DC0009:en:NOT

[50] Ibid.

not good enough since it leads to fragmentation and lack of harmonisation the Commission proposes a tougher notch up, a Regulation…for all areas of data protection except the police, where it seems that we would not mind the fragmentation and harmonisation that is inevitable if protection is only at the level of a Directive. The ordinary European citizen, never mind the legal scholar and other observers would be forgiven for thinking and asking "Where is the logic in this?"

The reader of the Commission's Communication is quickly assailed by more attacks on any sense of logic and is presented with another argument in favour of a Regulation:

"Individuals' rights must continue to be ensured when personal data is transferred from the EU to third countries, and whenever individuals in Member States are targeted and their data is used or analysed by third country service providers.

This means that EU data protection standards have to apply regardless of the geographical location of a company or its processing facility."[51]

Yet, as in other cases, the reader is compelled to reasonably ask "But why do these standards of uniformity not apply when it comes to personal data collected and used for police purposes?"

The question was asked by the present author in person to Mme Francoise le Bail[52] in front of several hundred participants at the CPDP conference in Brussels on 26 January 2012 to which she replied to the effect that Police issues were previously third pillar and thus outside the remit of EU law so to go straight to a Regulation would have been too big a step. The Commission decided to go a bit more slowly , one step at a time and in the case of the police use a Directive and not a Regulation. This would perhaps have been slightly plausible to a less informed audience but as it happened the author had just then already completed (September-November 2011) an advanced draft of a report on the implementation of Council of Europe Recommendation R(87)15 on the processing of personal data for police purposes across 21 European states[53]. So the answer provided by Mme Le Bail sounded suspiciously like a smoke-screen since all this talk of third pillar was simply EU-speak that did not reflect the reality on the ground i.e. that, as established in fact 7 *supra*, Europe and especially the Schengen countries had been going through a harmonization process in data protection in the police sector for the best part of a quarter of a century before the European Commission went public with the DPRP in January 2012. Moreover there was simply no excuse for the European Commission not to have known

[51] Ibid.
[52] Director General Justice at the European Commission

[53] "Recommendation R (87) 15 – Twenty–five years down the line" Report by Professor Joseph A. Cannataci and Dr. Mireille M. Caruana first submitted on 12 November 2011 with a revised version eventually later submitted on 26 September 2013 for consideration by the Council of Europe's Consultative Committee on Data Protection T-PD; Since completed with data from 31 European states and presented in person to the T-PD Plenary session on 15th October 2013. Officially restricted and due to be formally published on-line by the Council of Europe after final corrections and proof-reading before end December 2013, this report was leaked to Statewatch by unknown persons in September 2013 following its being made available to T-PD members. That 26 September 2013 version is available at http://www.statewatch.org/news/ and specifically downloadable at http://www.statewatch.org/news/2013/oct/coe-report-data-privacy-in-the-police-sector.pdf

about the results of the survey carried out on behalf of the Council of Europe by the PUPIE project throughout 2011 for the preliminary results were presented in some detail at the International Data Protection Conference held on the 21st September 2011 in Warsaw and again in even greater detail to all delegations from the 47 member states present at the plenary session of the T-PD Consultative Committee on Data Protection in Strasbourg held between the 28 November and the 01 December 2011. It is hard to imagine that the European Commission's delegation to the T-PD did not report back on 74 pages of the preliminary report available for the T-PD meeting of Nov-Dec 2011 which showed in no uncertain way that Rec(87)15 had had an impact over the 25 years since 1987 not dissimilar to that which would have been achieved by an EU Directive in the police and criminal justice sector. To be sitting on that evidence and then claim that data protection law was something new to the police sector in EU states was simply not credible.

In the days and weeks following the publication of the DPRP it became clear that before and after Christmas 2011 the EC's internal inter-service consultation, allegedly heavily influenced by lobbyists and the United States' representations resulted in a marked watering down of the draft Regulation's provisions when it was published officially on the 25th January 2012.[54]

The Commission furthermore appears to have reflected the position of the Council more than the European Parliament in the strategy it pursued when putting the Data Protection Reform Package (DPRP) together. This is perhaps why, rather than following the logic of one comprehensive legislative package pegged at Regulation level – as clearly preferred by the leading MEPs involved[55] it chose to divide the DPRP into a Directive regulating the Criminal Justice and law enforcement sector and a Regulation covering everything else. That it did so in a controversial manner especially in the way the provisions regulating some sectors (eg medical data etc.) appeared half-baked or other aspects ill-thought out (the powers delegated to the Commission) was reflected by over three thousand amendments tabled on the draft Regulation alone with over another thousand tabled on the draft Directive. The perpetuation of the fragmentation that the reform package had ostensibly set out to remedy was remarked upon by a number of analysts and especially those representing civil society

> "The original aim of the Commission was to create "a comprehensive personal data protection scheme covering all areas of EU competence," which would "ensure that the fundamental right to data protection is consistently applied". Instead, however, the current proposals would perpetuate a seriously fragmented system of

[54] "Apparently, significant reservations regarding the Commission's approach emerged within the data processing economic sector and during the consultations with the United States. In an "informal note", the US administration particularly criticised the introduction of new protection instruments (data breach notification, right to be forgotten, protection of children's data), the regulation of data transfers to third countries, and the requirement to obtain the authorisation of the competent supervisory authority prior to any disclosure of personal data upon the request of courts or authorities of third countries (Art 42 (2) of the draft).11 The impact of this criticism cannot be determined from the outside. Certainly, the version that was eventually adopted differs from the November 2011 draft in some important aspects. This includes especially the age of consent for children, which has been lowered from 18 to 13 years (Art 8 (1) GDPR; this corresponds with US legislation) as well as the deletion of Art 42 of the draft (a weakened provision is now contained in Recital 90)." Gerrit Hornung in "A General Data Protection Regulation for Europe? Light and Shade in the Commission's draft of 25 January 2012", ScriptEd Volume 9, Issue 1, April 2012, page 66 last accessed on 24 September 2013 at http://script-ed.org/?p=406

[55] "The rapporteurs also acknowledged they would have liked to get some additional features, starting from a uniform data protection regime for the private and public sector including law enforcement. The directive will allow member states to implement their own version of the legislation within a set of minimum standards. Data transfers within the EU therefore could again mean, that citizens from a country with higher standards might lose some protection when data is transferred beyond the border of their country." As reported by Monika Ermert, EU data protection: bumpy piece of road ahead, Internet Policy Review 24 October 2013 last accessed on 29 October 2013 at http://policyreview.info/articles/news/eu-data-protection-bumpy-piece-road-ahead/209

> data protection rules (albeit with greater harmonisation in some areas)… this continued fragmentation is neither necessary nor desirable. Intellectually and in terms of constitutional/fundamental rights law there is no reason why all processing of personal data subject to EU law should not be subject to one set of overarching basic rules. Moreover, the Regulation (including the restrictions and exemptions contained within it) is perfectly suitable to that end."[56]

Both the Article 29 Working Party and the European Data Protection Supervisor[57] in March 2012 overall welcomed the Draft Regulation, whereas they strongly criticised the Draft Directive which is regarded as being greatly inferior to the Draft Regulation. This level of criticism again begs a number of important questions: why is the police and justice sector being handled differently and separately from other sectors? Why does the current (1995) data protection directive allegedly lead to fragmentation to the extent that in 2012 the Commission proposes a Regulation to replace it yet at the same time, almost in the same breath, in 2012 it is proposing that the Police and Criminal Justice sector be regulated by a Directive?

In April 2012, in response to criticism that the DPRP has too many loopholes with the draft Directive being a major source of concern, the Commissioner responsible provided another rather lame explanation as to why the Police and Criminal Justice sector is proposed to be covered by a separate Directive and not the General Regulation . ""You need some kind of flexibility because police and security agencies do not function in the same way in all our countries yet," EU justice commissioner Viviane Reding told press in Brussels".[58] From a logical point of view this statement is quite baffling since if police and security agencies do not function in the same way in all EU countries the solution is clearly not to dispense with the clarity and uniformity of a Regulation but rather give a longer lead time for the introduction of the Regulation in order to permit all EU states to prepare themselves and make the necessary changes required by the a new Regulation. Reding would have been more credible had she said something like "Listen, there is no political will in the Council at this moment in time to have harmonization of data protection laws in the Police sector through a Regulation … and if I insist on having everything nice and logical all tied up in one Regulation – the much-awaited single set of rules on data protection, valid across the EU – then the governments on the Council will block everything so having a Regulation and a Directive may not be ideal or logical but it's better than nothing, better than no improvement at all". As it is Mrs Reding understandably did not come clean on all the problems faced both at the inter-service consultation and in the private sounding out of Council members that had been taking place for months. With that realization that we are not being told the whole story one might as well stop pursuing the path of logic and instead turn to documenting some of the instances where it appears to have been convenient for one or more EU governments to forget – or otherwise ignore - the facts.

---

[56] EDRI Position paper last accessed on 24th September 2013 at http://protectmydata.eu/topics/fragmentation-of-the-data-protecion-framework/

[57] Opinion of the European Data Protection Supervisor on the data protection reform package, 7th March 2012 Last accessed on 29th October 2013 at https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-03-07_EDPS_Reform_package_EN.pdf

[58] Nikolaj Nielsen, Police largely exempt from data protection directive, EU Observer 23 April 2012 last accessed on 29th October 2013 at http://euobserver.com/justice/115999

Forgetting (or ignoring) the facts

It is not only the European Commission which appears to have forgotten – or at best ignored – the facts as to the real status of data protection law in the police sector across Europe. The relevant reports from some of the Governments and/or Parliamentary bodies around Europe make for some remarkable reading. Restrictions of space do not permit an exhaustive survey of such instances but if a prize for obfuscation were to be awarded, in this case when discussing the DPRP, then the UK may probably be immediately declared to be the winner:

> "The Government shares the Committee's view that there is not a pressing need to update the Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters. The Framework Decision has yet to be fully implemented across all Member States, or evaluated. Implementation and evaluation of the current legislation should come first before new legislation is considered".[59]

This assessment by the UK Government ignores or forgets a number of significant facts:

i. That Framework Decision 2008/977/JHA had been heavily criticised by amongst others the European Data Protection Supervisor (EDPS) as not being fit-for-purpose since it only regulated exchanges of police data between EU states but not the processing of police data within each EU member state. So putting up an argument that it had not been fully implemented across all Member States is just plain nonsense since the real measure should have been "Is 2008/977/JHA/ up to the task of regulating police use of personal data in the UK and in all other EU member states across Europe?"

ii. That the principles of 2008/977/JHA to a considerable extent had been inspired by Rec(87)15

iii. That the UK had been represented at exactly the same Warsaw and Strasbourg meetings in 2011 and was in receipt of the same 74-page preliminary report as the European Commission and therefore should have been perfectly well aware of the facts about the true extent of the spread of data protection law in the Police sector during the 25-year run-up to the DPRP, thanks to the impact of Rec(87)15; So "implementation and evaluation of the current legislation" had actually already occurred in many instances across Europe often to a level higher than that of 2008/977/JHA but at a level of detail following the principles laid down in Rec(87)15

iv. That in its response and consideration in this instance the UK Government nowhere appears to have seriously considered pertinent factors such as the actual status of ease of transfer of police data, automated transfer and analysis as well a whole raft of new incoming trends in

[59] Government response to Justice Select Committee's opinion on the European Union Data Protection framework proposals Presented to Parliament by the Lord Chancellor and Secretary of State for Justice by Command of Her Majesty, January 2013 last accessed on 29 October 2013 at http://amberhawk.typepad.com/files/blog-uk-government-response-to-justice-re-eu-data-protection-proposals.pdf

the transfer of evidence in electronic form, all of which are state-of-the-art targets of harmonisation of data exchanges for LEAs across Europe.

If in nothing else however, the UK response was searingly and brutally honest in its conclusion "The Government therefore does not consider that full harmonisation of police and judicial co-operation in criminal matters is necessary or desirable"[60] The UK's views on what is desirable clearly ought to be respected but it would have been helpful if the arguments for necessity or lack of necessity would have been made in a more detailed and more persuasive manner. Instead the impression one gets on reading the UK response document is that "If one were to accept to harmonise on this matter with the rest of Europe then we would have to change the way we do things…and we'd rather carry on with our British way of doing things, thank you very much." The reader will judge if that is an appropriate attitude to take in the face of the fourteen facts and the risks outlined at the beginning of this paper and contrast that with say, the German attitude which in some instances appears to be motivated by a preference for the harmonised rules to be even stricter and more protective of individual citizens.[61] To be fair to the British, the Germans too had a number of reservations about the desirability and necessity of the Directive's approach to harmonization "The draft directive would therefore lead to far-reaching encroachments on criminal procedural law, which are not necessary in order to facilitate mutual recognition of decisions and cooperation in criminal matters with a cross-border dimension."[62] While this statement may be arguable in the light of growing computerization of court systems around Europe, it does show that the Germans may in their own way be just as protective of their own way of doing things as the British and the French to mention but two other major European states.

The inevitable conclusion pre-Snowden

The analysis so far leads one to conclude that the split into a Regulation and a Directive defies legal logic and does not take the 25 years of harmonization of data protection in the police sector achieved by Rec(87)15 into account. The development of the different drafts available of the Draft Directive before and after its formal publication in January 2012 further reinforces the impression that the current two-part proposal is far more likely to be the untidy result of behind-locked-doors compromise spurred by political imperatives than it being the result of impeccable legal logic. It is beyond the scope and space limitations of this paper to examine the DPRP on a section by section basis but it would be fair to say that while the Regulation is, if further tightened up, capable of being a significant step forward in some

[60] Government response to Justice Select Committee's opinion on the European Union Data Protection framework proposals Presented to Parliament by the Lord Chancellor and Secretary of State for Justice by Command of Her Majesty, January 2013 last accessed on 29 October 2013 at http://amberhawk.typepad.com/files/blog-uk-government-response-to-justice-re-eu-data-protection-proposals.pdf

[61] Data protection rules delayed at EU summit talks" EurActiv 25 October 2013 last accessed on 29 October 2013 at http://www.euractiv.com/specialreport-digital-single-mar/france-germany-form-anti-spy-pacnews-531306

[62] In its 895th session on 30th March 2012, the Bundesrat adopted Decision 51/12
Decision pursuant to Article 12, Point b, TEU:30 March 2012 last accessed on 29 October 2013 at http://www.google.com.mt/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&ved=0CC8QFjAA&url=http%3A%2F%2Fwww.ipex.eu%2FIPEXL-WEB%2Fdossier%2Ffiles%2Fdownload%2F082dbcc53782a3ff01378425d0850186.do&ei=1pJwUuvWEIKVtQann4DoAQ&usg=AFQjCNFcQGoMvpA165PDcpnwMPM4E1FtWg

areas, the Directive would only represent a tiny step forward in terms of substantive content or further harmonization in the case of LEAs and none at all insofar as SIS are concerned. Moreover, if asked point blank by a constituent, an MEP would have to honestly respond that neither the Regulation and especially not the Directive can be satisfactorily used to provide adequate safeguards against the type of mass surveillance revealed by Snowden since the EU cannot stray into matters of national security.

If this assessment is accurate then the ordinary citizen would be forgiven for asking how useful is the DPRP and why would anybody and especially several dozen or hundreds of MEPs vote it into being? The answer lies in the fact that the MEPs would be making a political calculation and not a legal one. If the MEPs were to throw the draft DPRP out at this stage they would be throwing the political baby out with the bath water. They would have nothing to show for their efforts on the subject for more than two years and it could be construed as a public admission of impotence by the European Parliament in the face of an EU Treaty which accords competence in matters of national security to national states – here read national parliaments – and not the European Parliament in Brussels/Strasbourg. Which Parliamentarian enjoys admitting his or her impotence to constituents, in any matter? So it is perfectly understandable if the MEPs would content themselves with some level of improvement through the Regulation, and some very modest harmonization with the Directive. While the latter would not necessarily achieve much that is substantive on the ground in the 28 member states since, as the PUPIE project results demonstrate, these all have the police use of personal data already regulated by law in line with R(87)15, it could conceivably contribute to some further harmonization and would anyway, in terms of EU law (as distinct from more generic European or national law) be an improvement over the spectacularly unimpressive CFD 2008/977/JHA which only covers data exchanges between LEAs in different countries and not the internal processing in each member state.

The way things were shaping up on the progress of the DPRP until May 2013 appeared to be a re-run of the *iter* of the 1995 Directive which was enacted at a time when many EU member states already possessed data protection legislation. Once Directive 95/46/EC came into force by 1998 many states did amend their legislation in an apparent attempt to comply with the new Directive but the result 14 years later, we are being told by the Commission in 2012, was so much fragmentation that now a Regulation is needed as opposed to a Directive. Likewise, if as WP 29 opines, in the case of the Police and Criminal Justice Sector, "a high level of consistent data protection standards also applying to this area is all the more needed'[63] it would be futile to ask if it is sensible to allow fragmentation to fester for another ten or fifteen years before taking more decisive action in the form of a Regulation. The calculation is clearly a political one and not a legal one.

[63] ARTICLE 29 DATA PROTECTION WORKING PARTY Opinion 01/2012 on the data protection reform proposals WP 191 Last accessed on29 October 2013 at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm#h2-2

The more recent developments– the LIBE vote and the European Council meeting of October 2013

By May 2013, unintentionally coinciding with the Snowden storm that was about to break, the European Commission and the Irish Presidency reacted to the torrent of requests for amendments to the DPRP by producing and publishing a "compromise text"[64] of the first four chapters of the Regulation. The Directive remained untouched by the Presidency for the time being.

While the vote of the LIBE Committee on the DPRP was postponed twice, when it came to the crunch on Monday 21st October 2013, it was clear that the two Rapporteurs, Albrecht and Droutsas had been assiduous in their preparation for the vote through meticulous preparation of a compromise text as a result of detailed negotiations with all the shadow rapporteurs of all the different groupings within the European Parliament. As a result, although there were over four thousand amendments overall, instead of the long-drawn out debate and vote, the LIBE Committee witnessed a near-record passage which lasted less than an hour. It is beyond the scope of this paper to enter into a detailed analysis of the resultant text after the LIBE vote. Suffice it to say that the LIBE Committee succeeded in beefing up a number of sections. It re-introduced the principle previously contained in the Art 42 which had been deleted by January 2012[65] so as per the current text, if "a third country requests a company (eg. a search engine, social network or cloud provider) to disclose personal information processed in the EU, the firm would have to seek authorisation from the national data protection authority before transferring any data. The company would also have to inform the person of such a request, MEPs say. This proposal is a response to the mass surveillance activities unveiled by the media in June 2013."[66] Likewise sanctions have been considerably increased and companies breaking the rules would face fines of up to €100 million or up to 5 % of the annual worldwide turnover, whichever is greater, as opposed to the penalties of up to €1 million or 2% of the global annual turnover as had been proposed by the Commission.

There has also been considerable criticism of the emergent text. EDRI summed it up as "One step forward, two big steps backwards" [67]claiming to be "shocked and disappointed that Parliamentarians voted to introduce massive loopholes that undermine the whole proposal."[68] Compromises 4, 6 and 20 were identified as being the most problematic parts of the text as adopted: "If allowed to stand, this vote would launch an 'open season' for online companies to quietly collect our data, create profiles and sell our personalities to the highest bidder" said Joe McNamee, Executive Director of European Digital Rights. "This is all the more disappointing because it undermines and negates much of the good work that has been done," he added. Despite almost daily stories of data being lost, mislaid, breached and

[64] 10227/13 Interinstitutional File: 2012/0011 (COD) dated 31st May 2013 Last accessed on 24 September 2013 at http://www.huntonprivacyblog.com/wp-content/uploads/2013/06/st10227-ad01.en13.pdf

[65] For a more detailed analysis of this point pls see. Cannataci, Joseph A. 2013. Concept paper on the application of data protection regulations in relation to transborder private/public information sharing for (a) network security purposes and (b) criminal justice purposes. Op.cit. infra. Unpublished paper commissioned by the Council of Europe produced in two versions December 2012 and September 2013, due to be published by the Council of Europe before 06 December 2013.pp22-26

[66] Civil Liberties MEPs pave the way for stronger data protection in the EU, European Parliament News 21 October 2013 last accessed on 29 October 2013 at http://www.europarl.europa.eu/news/en/news-room/content/20131021IPR22706/html/Civil-Liberties-MEPs-pave-the-way-for-stronger-data-protection-in-the-EU

[67] Data protection vote – one step forward, two big steps backwards | EDRI 21 October 2013 last accessed on 29 October 2013 at http://www.edri.org/eudatap_vote

[68] Ibid.

trafficked to and by foreign governments, our elected representatives adopted a text saying that corporate tracking and profiling of individuals should not be understood as significantly affecting our rights and our freedoms. The Committee extended the range of circumstances in which companies can process an individual's data without their consent - and made the rules far less easy to understand."[69]

The MEPs and the Commission were clearly pleased with the result of the vote and the mandate to negotiate on behalf of the Parliament with the Council[70] but the joy was to be short-lived since within three days it became clear that the prospects of an agreement being reached with the governments of the member states before the European Parliament elections in spring 2014 were close to zero.

The attempts to bring forward the implementation of the DPRP at the 24-25 October meeting of the European Council[71] "strongly pushed by France and the European Commission in advance of the summit– foundered however, with a new commitment to introduce the rules by 2015."[72]. This latest development would probably scupper the hopes of the MEPs and especially those like LIBE rapporteurs Albrecht and Droutsas who have openly campaigned for the DPRP to be adopted before the May 2014 European elections, no doubt also expecting that such legislative progress would enhance their chances of being re-elected. It would appear that the UK led a rival camp to the French at the summit[73] and that "Cameron had fought hard for the 2015 date, and began the summit negotiations arguing that it would be better to have no deadline at all."[74] The German position was pivotal and also supported a delay to the DPRP but for quite different reasons. In Merkel's own words "The UK wanted to delay the DPR because they feel that it may harm the interests of business," she said after the summit. "Germany had reservations on not moving too quickly to ensure that it can reconcile the existing rights of its citizens,"[75] she explained. Some observers have been quick to question if Merkel is not as keen on privacy as she may say "Chancellor Merkel has put on a good show of being outraged by American spying. But, at the same time, she has impeded efforts to strengthen data security. Does she really want more privacy, or is she more interested in being accepted into the exclusive group of info-sharing countries known as the 'Five Eyes' club"?.[76] Yet few observers have remarked that Merkel's position on the DPRP should come as no surprise given that she was completely consistent with what the German Minister of the Interior, Hans Peter Friedrich had stated two days earlier just after the DPRP was passed by the MEPs of the LIBE Committee in the evening of Monday 21st October at near-record speed. Friedrich clearly hinted that the

[69] Ibid.
[70] Frances Robinson, European Parliament Acts Quickly to Pass Data-Protection Vote. 21 October 2013, last accessed on 29 October 2013 at http://blogs.wsj.com/digits/2013/10/21/european-parliament-acts-quickly-to-pass-data-protection-vote/
[71] As distinct from the Council of the European Union or the Council of Europe
[72] Data protection rules delayed at EU summit talks" EurActiv 25 October 2013 last accessed on 29 October 2013 at http://www.euractiv.com/specialreport-digital-single-mar/france-germany-form-anti-spy-pacnews-531306
[73]" Data protection: France, UK lead rival camps at summit" EurActiv 24 October 2013 last accessed on 29 October 2013 at http://www.euractiv.com/specialreport-digital-single-mar/france-uk-lead-rival-data-campsnews-531283
[74] Data protection rules delayed at EU summit talks" EurActiv 25 October 2013 op.cit. last accessed on 29 October 2013 at http://www.euractiv.com/specialreport-digital-single-mar/france-germany-form-anti-spy-pacnews-531306
[75] Ibid.
[76] Gregor Peter Schmitz, "Appearances and Reality Merkel Balks at EU Privacy Push"Spiegel on-line 28 October 2013 last accessed on 29 October 2013 at http://www.spiegel.de/international/europe/germany-impedes-eu-privacy-efforts-despite-outrage-at-nsa-spying-a-930488-druck.html

DPRP as approved by MEPS on the 21st October needs to be changed to reflect the high German standards of data protection and at the same time providing reasonable responses to the challenges of the Internet age.[77] This German reluctance to go forward with the current texts is consistent with the reservations expressed by the Bundesrat and a number of analysts, some of whom may wish to beef up precisely those weaknesses highlighted by EDRI and referred to above. The effect that such a delay in the adoption of the DPRP may have is more properly understood in the context of other developments considered in the concluding section below.

Conclusions

Long before the Snowden storm broke, it was clear that the DPRP and especially the decision to split he exercise into two legal instruments defied all legal logic as well as the stated purposes of an exercise aimed at de-fragmenting the European personal data legal eco-system. The statements made by some of the leading actors suggest that the facts about the real state of European data protection laws regulating the use of personal data by LEAs were inadvertently overlooked, conveniently forgotten or, in the worst case deliberately ignored. It clearly did not suit the negotiating position of countries such as the UK nor the political agenda of the European Commission to acknowledge that in 2012 European states had already lived through a quarter century of harmonization of its data protection laws in the police sector and perhaps none more so than the member states of the EU in the Schengen area which had long adopted the principles of R(87)15 as part of the *acquis comunitaire*. The lesson drawn from these observations is not a novel one: it is futile to look for legal logic or indeed just plain common sense when one should be looking for the best that could be achieved in a situation where the law-making process is manifestly primarily driven by political expediency rather than what's actually sensible and appropriate. The DPRP was never going to be anything better than the result of political compromise, indeed a number of political compromises.

Even if one were to accept the proposition that the DPRP as published in January 2012 would be an improvement on the current situation in some areas but not entirely fit-for-purpose, a consideration of the fourteen pertinent facts and the associated risks as outlined above in the wake of the Snowden revelations very strongly suggests that the proposed legal solution within the current version of the DPRP as amended up to 21st October 2013 is grossly inadequate to deal with the massive intrusion on privacy constituted by the activities of SIS. The way that things work in practice and especially the extent of information-sharing that takes place in many states between LEAs and SIS means that it is hopelessly inadequate to have a legal framework aimed at LEAs alone. That adequate legal safeguards are needed to protect citizens from potentially abusive SIS activity is as clear that those safeguards are

[77] Konrad Lischka, Friedrich will Datenschutzregeln wieder ändern, Der Spiegel on-line, 22 October 2013 last accessed on 29 October 2013 at http://www.spiegel.de/netzwelt/netzpolitik/eu-datenschutzverordnung-innenminister-friedrich-kritisiert-regeln-a-929196.html Friedrich's position is in substance consistent with that of the Bundesrat as expressed in 2012 and there are various areas which can be improved in the DPRP. Additionally, the German Interior Minister, who hails from the CSU party, would presumably not be overly upset if any delays he forces onto the DPRP would possibly be construed as a setback for another German politician from a rival party, the Greens, the MEP Jan Phillip Albrecht who had previously called for his resignation.

largely nowhere to be found in the DPRP. The re-introduction of the old Article 42 into the Regulation is simply not enough to reassure anybody that a solution has been found to NSA/GCHQ-style mass surveillance. The limitations placed on the European Union by Article 4.2 of the EU Treaty excluding its competence on matters of national security suggest that if a legal solution to the problem is to be found in the short to mid-term this is not to be sought within the formal framework of the institutions of the EU. Submitting a resolution to the General Assembly of the United Nations[78] is not going to solve the problem either so other options for legal solutions may be considered.

It is not clear what will be the outcome of the recent calls by Germany and France for the USA to come to an agreement with them about activities of intelligence agencies by Christmas 2013[79]. It is unlikely that membership of the Five Eyes partnership would be offered to placate them nor is it likely that such a development would be a satisfactory solution for both France[80] and Germany[81]. Both of these major European powers are sensitive to the fact that a lasting solution can only be achieved by tackling the issues within a much broader context and will seek to protect their national as well as European interests by widening their appeal to a much wider international audience ostensibly taking the BRICS nations into account.

Under the circumstances, the most obvious forum for taking the legal discussion forward is the Council of Europe (CoE) in Strasbourg where a binding legal instrument such as a multi-lateral treaty or convention can be usefully debated and drafted. In a matter which primarily revolves around human rights and a right to data protection founded on the basis of the right to private and family life, the Council of Europe has the best possible pedigree and track record in the field of human rights and data protection where its activities have preceded those of the European Union by over twenty years. The Council of Europe has also proven to have the credibility and the ability to create international consensus far beyond the borders of Europe as most emphatically demonstrated by the United States and other non-European states ratifying the Cybercrime Convention created through the initiative of the CoE. The Council of Europe not only has a much wider membership than the EU thus automatically

[78] Colum Lynch, John Hudson, Shane Harris "Exclusive: 21 Nations Line Up Behind U.N. Effort to Restrain NSA" 25th October 2013 last accessed on 29th October 2013 at http://thecable.foreignpolicy.com/posts/2013/10/25/exclusive_21_nations_line_up_behind_un_effort_to_restrain_nsa

[79] Data protection rules delayed at EU summit talks" EurActiv 25 October 2013 op.cit. last accessed on 29 October 2013 at http://www.euractiv.com/specialreport-digital-single-mar/france-germany-form-anti-spy-pacnews-531306

[80] "François Hollande, the French president, expressed no desire to join in such an intelligence-sharing arrangement, saying his country's spy agencies were happy to operate independently. "We're not within that framework and we don't intend to join," Mr Hollande said. "France is a European country, it's part of this alliance, and is an independent country when it comes to making choices and making decisions." Extracted from Peter Spiegel "Angela Merkel eyes place for Germany in US intelligence club" FT-Weekend 25 October 2013 last accessed on 29 October 2013 at http://www.ft.com/cms/s/0/e2492a3a-3d7a-11e3-9928-00144feab7de.html

[81] "Jan Techau, a former German defence ministry official who heads the Carnegie Europe think-tank, said he believed the US will be unwilling to change its approach to Germany, despite the current scandal, because of deep-seeded scepticism about German national interests. "Despite Germany being a key ally, there was, and is, a great deal of US mistrust in Germany over its perceived softness on Russia, its ties with Iran, and its close economic relations with China," Mr Techau said. "This mistrust is not entirely gone and as long as it persists, such agreements might actually be worthless." Extracted from Peter Spiegel "Angela Merkel eyes place for Germany in US intelligence club" FT-Weekend 25 October 2013 op.cit. last accessed on 29 October 2013 at http://www.ft.com/cms/s/0/e2492a3a-3d7a-11e3-9928-00144feab7de.html

bringing important states like Russia into the discussion. It has also over the years demonstrated the flexibility to move forward and achieve satisfactory solutions without the whole process being bogged down by the reluctance of one country to play ball. Neither France or Germany, nor indeed any other European state are expecting the UK to take a lead in this matter and this is not simply because the close relationship between its GCHQ and NSA or because its membership of the Five Eyes makes it odd man out in Europe. The UK has historically never been very keen on harmonizing its laws with those of the rest of Europe in matters relating to data protection in the sector of police and criminal justice administration. Its current position comes as no surprise to those observers who watched it first delay and then distance itself from the Council of Europe's R(87)15 over a quarter of a century ago[82]. The additional advantage of the CoE in Strasbourg as a forum is that, unlike the EU, it has the competence to negotiate an international treaty taking the activities of SIS and national security into account and has the institutional capacity to do so even if the UK or indeed any other member state does not wish to be part of such a process. The views of the UK and indeed those of any other dissenting members will as ever be listened to very respectfully and indeed, if it chooses to do so, the UK can contribute a great deal in a constructive manner. It is not in this instance however in a position where it has the credibility to take the lead in brokering a satisfactory deal with the United States and other non-European countries.

Reading the runes, although the French still have the ability to surprise, all the available evidence points to Germany being the country which will take the lead and push at the highest levels for the Council of Europe to take the bull by the horns and seek an international treaty regulating the activities of SIS. The personalities and track record of some of the actors involved also indicate more common ground than at first meets the eye. The final form of the German cabinet will depend on the outcome of the negotiations between the CDU/CSU and the SPD so it is as yet uncertain as to whether the current German Minister responsible for the Interior, Hans Peter Friedrich will be confirmed in post. Perhaps especially if he is so confirmed, we can certainly look forward to some interesting developments. The 29-year old Green MEP who was the EU LIBE Committee's rapporteur for the Regulation part of the DPRP, Jan Philip Albrecht, also a German national, has cast doubt on Friedrich's credibility in the wake of the Snowden affair[83]. Albrecht has made a very positive contribution within the European Parliament throughout his work as rapporteur but in this case he may wish to look deeper into the complexities of the situation and may possibly come round to the view, albeit possibly only in private, that, however vague at times, Friedrich may have been right all along. For the German minister of the interior had

[82] 1. When this recommendation was adopted: in accordance with Article 10.2.c of the Rules of Procedure for the meetings of the Ministers' Deputies, the Representative of Ireland reserved the right of his Government to comply with it or not, the Representative of the United Kingdom reserved the right of her Government to comply or not with Principles 2.2 and 2.4 of the recommendation, and the Representative of the Federal Republic of Germany reserved the right of his Government to comply or not with Principle 2.1 of the recommendation;

[83] "Jan Philipp Albrecht, a Green MEP, said Friedrich had spent the past few months blocking block efforts for tighter data protection regulation at European level, favouring self-regulation over a tightening of rules in Brussels. "The interior minister has not only failed to act in Germany's interest, he also failed to act on Angela Merkel's promise to take data protection more seriously," he said…. In June Friedrich said the NSA scandal was driven mainly by "a mix of anti-Americanism and naivety". But on Thursday the interior minister told the Leipziger Volkszeitungnewspaper that America should apologise for its actions: "Bugging and snooping on friends in public or in private is unacceptable." Albrecht said the affair was a huge embarrassment for the Christian Democratic Union politician and should rule him out from continuing in the same post in a new government: "I ask myself: why is this man still interior minister?" extracted from Philip Olterman "Angela Merkel bugging claims met with schadenfreude in Germany"The Guardian, 24th October 2013 last accessed on 29 October 2013 at http://www.theguardian.com/world/2013/oct/24/angela-merkel-bugging-schadenfreude-us-nsa-surveillance

publicly outlined a vision that sought a solution in something akin to an “on-line bill of rights”. “And, I believe, we need a kind of "charter of basic rights" on privacy protection and data sovereignty”[84] As part of this “charter of basic rights” Friedrich has gone on record to state that “On the one hand, the clear answer and I believe also a message to the United States should be: We want to protect our citizens' self-determination for their data! The most important element of this is transparency.”[85] Compare this statement with the very first principle enunciated in President Obama’s Consumer Privacy Bill of Rights “1. Individual Control: Consumers have a right to exercise control over what personal data companies collect from them and how they use it.”[86] All of which seems to be completely consistent with the German constitutional principle of informational self-determination. Friedrich’s political acumen would no doubt have suggested to him that he would need every bit of existing common ground possible in order to have the beginnings of a chance to achieve a breakthrough consensual position with the United States about re-writing the rules of engagement about surveillance and national security.

So whereas Friedrich wittingly or unconsciously found common ground with President Obama whose digital Bill of Rights of 23 February 2012 actually enunciated principles which are quite close to the German constitutional principle of informational self-determination, Friedrich linked this substantive approach to issues linked to next steps regarding on-line security. “Secondly, we want to develop a common understanding about data security in conjunction with our American friends”. Whether he places it in the context of a Charter of Rights or otherwise, Friedrich can read the political and popular moods well and knows that nothing short of a binding agreement which includes transparency as one of the primary safeguards would satisfy current expectations inside Germany and across much of Europe. A new International Cyber-Authority created by a new Council of Europe Convention on Cyber-Security would be able to provide the transparent operation and multiple safeguards giving credence to a newly-recognised international right to informational self-determination. Moreover in July 2013 Friedrich was already clearly rooting for the re-introduction of Article 42 of the draft Regulation pre-empting the tightening of the DPRP through the re-introduction eventually approved by LIBE on the 21st October 2013. “What happens to the data that I surrender to someone in public, in private or for financial purposes? Which legal measures can I use to create a framework to keep this safe? First of all through the Data Protection Directive, that is, with laws that should apply to all of Europe, in particular to corporations and also to the large American telecommunication companies. Here we demand that when companies hand over data from European or German citizens to American agencies, they also be required to inform about and report this. I believe this to be a mandatory part of transparency.”[87]

The new dimension that the Snowden affair brings to the argument is that a new legal solution would not only look at individuals in their role as consumers but also as citizens of states where SIS like LEAs have important but legally circumscribed roles. Taking the initiative by regulating these matters through

[84] Bernd Riegert / sad, “Interior Minister: 'Too much secretmongering'” An interview with Hans-Peter Friedrich, Deutchse Welle, 20 July 2013 last accessed on 29 August 2013 at http://www.dw.de/interior-minister-too-much-secret-mongering/a-16963590
[85] Ibid.
[86] Last accessed on 29 October 2013 at http://money.cnn.com/2012/02/23/technology/privacy_bill_of_rights/index.htm?iid=EL
[87] Bernd Riegert / sad, “Interior Minister: 'Too much secretmongering'” An interview with Hans-Peter Friedrich, Deutchse Welle, 20 July 2013 op.cit last accessed on 29 August 2013 at http://www.dw.de/interior-minister-too-much-secret-mongering/a-16963590

an international treaty open to all countries in addition to the United States makes practical sense in a world rendered borderless in cyberspace by the Internet. Obama also has his own national constituency to satisfy. The Snowden revelations have not only led to issues with the USA's allies overseas but also to considerable dissatisfaction at home over excessive surveillance on US citizens. Working on the legal dimensions of a solution that would also help make the Internet a safer place for US citizens wherever they are would be something that could earn Obama and the Democrats kudos on the domestic front too.

Moreover both President Obama on the one hand, as well as Friedrich and Merkel on the other hand, not to mention Hollande, would probably not be blind to the possibility of writing their name in history as being the prime movers of the first international treaty which effectively does to cyberspace that which the 1968 Non-Proliferation Treaty[88] did to nuclear weapons or the 1993 Chemical Weapons Convention Treaty[89] did to the non-proliferation of chemical weapons. For a new multilateral convention aimed at creating a more privacy-friendly environment for citizens in cyberspace without compromising national or international security is actually also an opportunity to re-write the rules of engagement about the activities of SIS and LEAs in cyberspace and, in technical terms this is by definition also an opportunity to outlaw cyber-war. The legitimate monitoring and surveillance mechanisms that could be agreed for cyberspace in the context of a new treaty aimed at preventing undesirable mass surveillance could also serve the purpose of detecting and eventually intercepting cyber-war attacks. In the same way as, say, the Organisation for the Prevention of Chemical Weapons (OPCW) and its Technical Secretariat helps keep the world clean from chemical weapons, a new International Cyber-Authority put into place by a new CoE Cyber-Security treaty could be given the means to credibly monitor internet traffic in a way which could help detect and eventually deter most forms of cyber-war. The very same type of intercept and monitoring software which is today allegedly used by the US, UK and German SIS could conceivably, through strict audit trails and international supervision be used to monitor the internet for forms of behavior which are internationally agreed to be off-limits whether this be child pornography or terrorist activity. Given the overlap that exists between serious organized crime and counter-terrorism and the functions of LEAs and SIS in such issues, it would appear sensible to accord an important role to organisations such as INTERPOL in the governance, auditing and possibly even the execution of the activities of a new International Cyber-Authority. Such an arrangement may certainly fit the bill for French President Hollande who "appears to be seeking a far narrower agreement that would require allies to inform each other if they were targeting nationals of their respective countries and barring the long-term storage of internet and telephony data of French citizens."[90] "François Hollande,

[88] Treaty on the Non-Proliferation of Nuclear Weapons signed 1 July 1968 came into force on 5 March 1970

[89] Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction signed 13th January 1993 came into force 29th April 1997

[90] Extracted from Peter Spiegel "Angela Merkel eyes place for Germany in US intelligence club" FT-Weekend 25 October 2013 op.cit. last accessed on 29 October 2013 at http://www.ft.com/cms/s/0/e2492a3a-3d7a-11e3-9928-00144feab7de.html

also called for a new code of conduct agreed between national intelligence services in the EU, raising the question of whether Britain would opt to join in."[91]

Is even contemplating the existence of a new International Cyber-Authority overly naïve? Perhaps not since in reality it serves nobody any good to have the internet used for activities such as organized crime, terrorism or paedophilia. It is not difficult to see all kinds of countries agreeing to come together over such a common goal. Nor would cyber-wars be desirable to all except for a few rogue states. So re-writing the rules of engagement in cyberspace would actually be eminently sensible from many viewpoints. The sticking point is not actually the declared goal of security but actually that of power or at least the perceived competitive edge that could be obtained in terms of industrial espionage or information about the negotiating positions of one's partners or competitors. Would the leaders of Germany and the USA recognize that, post Snowden, creating and retaining international trust is much more important and valuable than any possible short-term negotiating advantage through covert surveillance on the internet? Given the results of the US presidential election in 2012 and the German elections of Sep 2013 the political leaders of both countries should feel strong enough to pursue sensible and legally logical choices. The consequences of failure in their efforts to do so would certainly not be as bloody as a failed intervention in Syria or disengagement in Iraq and Afghanistan. The possibilities of success and their implications for prosperity in the continued economic success of internet activity are alluring.

Even more so if Obama *et al* may follow the thinking of former US Deputy Under Secretary of Commerce for International Trade Policy and Development David Rothkopf, "That in turn frames a question that I heard asked often when I was in Bill Clinton's administration and have heard not infrequently subsequently: Is the intelligence we might be gathering worth the risks entailed by getting it? I acutely remember a very uncomfortable meeting with a number of very senior-level officials in which this question was raised about economic intelligence in particular. The conclusion of the intelligence official in attendance was that it was not. We have now started to see similar questions raised about the benefits of this latest wave of spying on friendly governments."[92] Once the perceived advantage of economic intelligence derived from cyber-surveillance is discounted, then the argument for open, transparent collaboration over cyber-security with international partners and especially Europe may become overwhelming. Like so many other clear-headed Americans, Obama may also heed Rothkopf's succinct insight "Watch closely as the NSA scandal accelerates the pace of cyber-nationalism and more countries start setting rules for the Internet within their borders that undercut the promise of free Internet and the political and economic benefits to the United States that might bring."[93] Friedrich,

[91] Ian Traynor, "Germany and France warn NSA spying fallout jeopardises fight against terror Angela Merkel and François Hollande lead push at EU summit to reshape transatlantic spying and agree new code of conduct" The Guardian 25 October 2013 last accessed on 29 October 2013 at http://www.theguardian.com/world/2013/oct/25/germany-france-nsa-spying-merkel-hollande-eu

[92] David Rothkopf "False Fronts How the biggest intelligence community scandal in modern memory and Washington's infamous Twitter troll expose the real D.C.", Foreign Policy 29th October 2013 last accessed on 29 October 2013 at http://www.foreignpolicy.com/articles/2013/10/23/false_fronts_natsecwonk_nsa_scandal_expose_washington?print=yes&hidecomments=yes&page=full

[93] Ibid.

Merkel and Hollande will be well aware that Obama would understandably wish to go for the bigger prize with the lower risk, i.e. the political and economic benefits of a free and open Internet and that would suit their domestic audiences as much as it would suit Obama's. A UN-sponsored treaty would forcibly involve more actors and, in relative terms, take too long to achieve[94] . Moreover, a UN-sponsored treaty at a later date would not in any way be excluded by a successful attempt to negotiate a Cyber-security treaty within the Council of Europe in the short-to-mid-term. There are plenty of examples where the UN has latched on to previous examples of good practice in international law and the case of cyber-space could be yet another one.[95] If before Snowden the activities of SIS were the elephant in the Internet room, in the post-Snowden areas the cross-border nature and the extent of activities of SIS have produced a veritable herd of elephants which can no longer be safely ignored. The meeting rooms of the Council of Europe in Strasbourg may yet become the favoured venue for identifying the various members of the herd and leading them out of the room to safer pastures while the rest of the world gets to use the Internet room as a safer and more privacy-friendly place. Such a development would not necessarily go down well with some people in Brussels where the DPRP was hatched, but, as ever, "Politics is the art of the possible" and the European politicians involved know all too well the limits of what the European Parliament and the European Commission can achieve before the Parliament is dissolved and new European elections are held in spring 2014.

MEPs involved in the DPRP are working to quite a different time fuse and marching to a different drum-beat than the leaders of Governments working in the Council of the European Union. Many of the latter and especially the Chancellor and Interior Minister of Germany are now very recently confirmed in the driving seat in their countries for the next 3-4 years at least and therefore do not share the same imperatives as MEPs whose term expires within six months in May 2014. It is likely therefore that the Ministers and leaders of Governments sitting on the Council of the European Union may be in no rush to agree to the DPRP before the May 2014 European elections and would use the Council of Europe as a more convenient and timely conduit for defusing the Snowden affair. That course of action would have the additional advantage of allowing new MEPs and a potentially revitalized LIBE, not to mention a largely new set of Commissioners, time to settle down and take their own positions about the DPRP. Unless it is perceived to be an indispensable form of leverage in the negotiations with the US over various matters, the discussion of the DPRP will therefore most probably continue throughout 2014-2015, by when the issue as to whether it should be a Regulation or a Directive will ultimately be re-visited and hopefully resolved. It is also not impossible that it would be resolved at more or less the same time that a new US-backed Council of Europe Convention on Cyber-safety and cyber-security would be approaching finalization. If the DPRP arguments are finally resolved in the direction of a Regulation then the inevitable formal and informal cross-fertilisation between the DPRP and the new convention might be very instructive. The discussion would possibly be more mature and objective than

[94] In terms of political time-fuses that is. It is not inconceivable for a Council of Europe convention to be negotiated in the space of 2-4 years if political will exists at the right levels. The Cybercrime Convention was negotiated in under four years between 1996 and 2000. This time-frame chimes best with the political lives of the US and German incumbents. A UN Treaty would probably take more like 5-7 years to put together.

[95] The Chemical Weapons Convention drafted by the 18-nation Conference on Disarmament, itself builds on the Geneva Protocol of 1925. The Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or other Gases, and of Bacteriological Methods of Warfare, signed in Geneva on 17 June 1925, is itself a protocol to the Hague Conventions of 1899 and 1907.

the one we have witnessed to date and the inclination to hive off police processing of personal data into a separate Directive may all but vaporise. To some observers that could signal the possibility of the disappearance of the currently proposed draft Directive for regulation of Police uses of personal data with its main provisions being instead finally and more sensibly integrated into the main text of a re-modelled and revised draft Regulation. If nothing else, such a development would certainly reflect a political judgement which is more respectful of legal logic and more well-tuned to the realities of the creation and use of personal data in the second decade of the 21st century. This of itself would not be so much worrisome as welcomed. In the same way that the Council of Europe led the way in the field of data protection since 1976 and this found its way into the EU *acquis communitaire* by 1995-98 through a process of national and international osmosis, so too would a new Strasbourg-led regime for cyber-space in due course percolate through to an EU-compatible form.

The alternative scenarios for a roadmap of information policy and governance for the Internet would possibly prove to be prohibitively expensive from a financial perspective and equally unattractive from a foreign policy point of view. For while the Council of Europe may have an unassailable edge in the field of human rights, an edge conferred by the CoE's focus and primary mission, it is the EU which has the remit for economic growth and the financial clout that goes with it. In other words, if Strasbourg-led initiatives on a new Cyber-security Convention were to fail, it is probable that the EU would have to, sooner rather than later, seriously study the prospect of going down the route of cyber-nationalisation and financing the building of what Eric Sadin has dubbed Web 3.0[96] or a European-controlled section of the Internet. If Fortress Europe were to also have its avatar in a real-life non-game version of Second Life, the discussion of a re-vamped DPRP would doubtless also be affected.

Odds on however that politicians on either side of the Atlantic would first work hard to prevent the further fragmentation of the Internet. This fragmentation would simply be too costly – though not impossible - in many ways. Which is why one won't be surprised to see history repeating itself. In the case of the drafting of the 2001 Cybercrime Convention, the Council of Europe had in 1996 been very careful to invite a host of influential non-member states including Canada, Japan and the United States to join the process from the very beginning. If in 2014 the Council of Europe would be led, most probably by German and French initiative, to create a working group with the task of drafting a new Convention for Cyber-security, then the list of invitees would probably very much resemble that of 1996 with the significant addition of the BRICS countries. With the Brazilians, the Russians, the Indians, the Chinese and the South Africans around the same table as well as the North Americans and the leading European powers not to mention the Australians and the New Zealanders, life could become very interesting indeed. One or more of the invitees may eventually walk off and discourage the others to the point where traditional distrust may ruin things irrevocably or on the other hand simply encourage the

[96] Eric Sadin, Après Prism, à l'Europe de créer un Web 3.0 responsable, Le Monde 22 October 2013 last accessed on 29th October 2013 at http://www.lemonde.fr/idees/article/2013/10/22/apres-prism-a-l-europe-de-creer-un-web-3-0-responsable_3501176_3232.html

others to redouble efforts, accept compromise and agree to a workable solution. The wiser countries will most probably recognize that the stakes are too high and that the probable consequences of non-agreement, the further “Balkanisation of the Internet” too unattractive a prospect to seriously contemplate. The related international cyber-law will follow suit.