Data protection in relation to transborder information sharing for network security and criminal justice purposes

Discussion paper

by Joseph A. Cannataci

Version 30 September 2013

This concept paper has been prepared by Professor Joseph A. Cannataci, for the Data Protection and Cybercrime Division (Directorate General of Human Rights and Rule of Law), within the framework of the Global Project on Cybercrime and the joint project CyberCrime@IPA of the Council of Europe and the European Union.

Professor Cannataci is Chair in European Information Policy & Technology Law, Co-Director STeP - Security, Technology & e-Privacy Research Group, Department of European and Economic Law, Faculty of Law, University of Groningen, The Netherlands; Head of Department of Information Policy and Governance, Faculty of Media and Knowledge Sciences, University of Malta; Adjunct professor, Security Research Institute & School for Computer & Security Science at Edith Cowan University, Australia; Associate, Cyber Security Center, Longwood University, USA.

The paper reflects the views of its author.

This research was commissioned by the Council of Europe and completed with support from

Executive Summary

Between November 2012 and September 2013, the author responded to a brief commissioned by the Directorate General of Human Rights and Rule of Law of the Council of Europe. The initial work carried out to end December 2012 was subsequently revised and up-dated over the period Jan-Sep 2013 to reflect the impact of the developments over the European Commission's Data Protection Reform Package (DPRP) and increasingly that of the revelations of the US whistle-blower Edward Snowden.

This study first examines some implications for data protection regulations in relation to transborder private/public information sharing for (a) network security purposes and (b) criminal justice purposes in the context of the Council of Europe's Recommendation R(87)15 on data protection in the police sector.

The concept paper identifies ten conclusions as at September 2013 and advocates that the time has come for a binding legal instrument which is capable of being deployed across sectors which have hitherto often been parallel worlds: that of law enforcement agencies (LEAs) and the other of Security & Intelligence Agencies (SIS). The concept paper takes into account the available evidence of utility of the EU's 2006 Data Retention Directive as well as the significance of the Snowden revelations for privacy & data protection.

These considerations reinforce the concept paper's recommendations that the Council of Europe (CoE) offers the right forum for one or more of at least three options which could produce a suitable new binding legal instrument: (1) an entirely new multi-lateral treaty or Convention which would contain mandatory provisions applicable to the LEA and SIS handling of personal data; (2) an additional protocol to the CoE's Data Protection Convention (ETS 108) encapsulating the provisions envisaged in Option 1 and/or (3) an additional protocol to the CoE's Cybercrime Convention (ETS 185) incorporating some of the provisions envisaged in Options 1 and 2.

The concept paper finds that the urgency for and the onus upon the CoE to take immediate action to produce a new binding instrument is compounded by the Snowden revelations and the possible chronic inadequacy of EU responses in the sphere of national security on account of exclusions of competence by Art 4 Section 2 of the EU Treaty.

Contents

1 Context of the Study

This study has been drawn up in the context of a consultancy contract between the Council of Europe represented by Mr Alexander Seger, Head of the Data Protection and Cybercrime Division, Directorate General of Human Rights and Rule of Law and Professor dr. Joseph Cannataci, Chair in European Information Policy & Technology Law, University of Groningen, The Netherlands, hereinafter referred to as "the Consultant".

2 Scope

The Consultant was requested to, in particular:

> prepare a 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.

The paper may be based on a scenario where a private sector entity in country A disposes of information (threat intelligence on IP addresses, malware found, geo-location data) on multiple computer systems infected by malware and forming part of a botnet in country B (and other countries). The entity in country A shares this information with an ISP in country B who then contacts its customers to help them clean their systems. Alternatively, the entity in country A may share this information with a CERT or similar in country B who contacts owners of the infected systems.

The concept paper is to address questions such as:

- Which data protection laws apply to the delivery of the information: the legislation of the provider of the information (country A), or the legislation of the receiver of the information (assuming here that both the entity receiving the information and the owner of the infected device are in country B)?

- If the law of the country of the infected device applies (country B), does it apply for the simple fact that the information is related to a person that can be identified in this country? Or will the law of the receiving country apply only in certain circumstances (for instance, when the provider of the information who is based in country A proactively establishes a connection to the infected device in country B)?

- Which entity is supposed to comply with the data protection law of the receiving country: the provider of the information (which is based in country A) or the receiver of the information (the ISP or the CERT based in country B)?

- If the information is delivered to country B for the exclusive purpose of helping to remove malware, is the provider (based in country A) of the information exempted from some or all obligations pursuant to data protection law of the receiving country (country B)?

- If the information is delivered for the purpose of supporting criminal investigations, is the provider (based in country A) of the information exempted from some or all obligations pursuant to data protection law of the receiving country (country B)?

When considering these scenarios the consultant is to consider existing international data protection standards (such as Convention 108 and Recommendation R(87)15 of the Council of Europe).

The consultant is also to include a short analysis of the implications of the proposed data protection package of the European Union regarding transborder private/public information sharing for purposes related to cybersecurity (protecting systems as in the scenarios above) and cybercrime (criminal justice investigations), including Recital 90 of the draft Regulation.

3 Structure of the study and background information

Given the constraints imposed by the contractual word limit, the main body of the study will only deal with background information and data where these are immediately pertinent to a point of analysis and/or a recommendation being made. The Consultant takes as a starting point the main data protection rules applicable to the case studies predicated in the brief i.e Convention 108 and Recommendation R(87)15 of the Council of Europe with a secondary consideration of existing and proposed EU legislation on the matter. Furthermore, the Consultant shall assume that the readers of this present study are familiar with five other recent studies that he has authored or co-authored[1]. Taken together, these five background papers should serve to bring relative newcomers to the area up to date with a number of privacy risks and relevant developments in police use of personal data to end September 2013.

The transmission of data held by the private sector to other actors in the private sector as well as to a Law Enforcement Agency (LEA) or a Security or Intelligence Service (SIS) or CERT whether within or across borders may occur in a variety of circumstances and some of these are here examined in outline form in order to provide more context to the specific questions set in the brief.

The bulk of this report was prepared by December 2012 when an interim first version was submitted and a pause was utilized to await developments in the EU data protection package being discussed within the LIBE Committee of the European Parliament. This latter process was and remains replete with uncertainties but seems also to have been overtaken by the impact of the revelations by Edward Snowden in and after May 2013. The contents of the original interim version of the report were reviewed in September 2013 in the light of these developments and revelations and two new sections added in order to take into account the impact of the "post-Snowden era" as further detailed in other sections below.

1 "Recommendation R (87) 15 – Twenty–five years down the line" Report by Professor Joseph A. Cannataci and Dr. Mireille M. Caruana submitted on 26 September 2013 for consideration by the Council of Europe's Consultative Committee on Data Protection T-PD;

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

4 Approach taken by the Consultant – R(87)15 & Conventions 108 & 185

The overall approach taken by the Consultant is that although the brief is understandably focused on data transfers within the context of Recommendation R(87)15[2] and Conventions 108[3] and 185[4], the efficacy of these three legal instruments cannot be measured properly if considered in a vacuum or if they are taken out of their proper context in European and international law. The proposals and recommendations made by the Consultant shall therefore at each step, bring to bear knowledge of developments in other areas of privacy and data protection law outside the immediate texts of R(87)15 and Conventions 108 and 185 but which would have a bearing on any attempts at improving these important instruments devised by the Council of Europe.

5 The context of data transfers to, from and within the private sector

The rule of law is very often built on the premise that what is "good for the goose is good for the gander". In Italian terms "La legge e uguale per tutti" (The law is equal for all). This is why, before proceeding to the case study scenario suggested in the brief, it is useful, especially if it is later required to reason by analogy, to examine the reach and background of current data protection law in the law enforcement sector and then reflect on the general nature of its applicability. The brief outlined in Section 2 above shall still be our point of departure however and especially that part which states that this concept paper shall focus "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."

It is essential to note that the all-important notion of purpose is to be found in both (a) and (b) above. Purpose, or *finalité* in its French incarnation, is the principle on which much of European data protection law is predicated whereby the collection and onward processing of personal data is only permissible if it is specifically for the stated legitimate purpose of its collection or, at minimum, a compatible purpose. This aspect of the present study deals with what has probably been one of the greatest changes in the realities of data protection law in the area of police use of personal data since the inception of R(87)15.

To better understand these developments and reflections it is useful to go back 26-28 years to the period of 1984-1986 when R(87)15 was being drafted and to examine the final results of the deliberations of the Council of Europe's Committee of Experts on Data Protection (CJ-PD) as it was then called. As explained in further detail in the background material referred to in the first footnote, one of the great innovations of R(87)15 is that it introduced the notion of purpose fairly and squarely into the sector of police use of personal data. Hitherto, the period 1981-1987 may be considered to be "the limbo years" for police use of personal data since many European police, security and law enforcement agencies interpreted the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS 108) as providing a blanket exception from the purpose provisions of data protection law. So, although Art.5 of the Convention provides that "Personal data undergoing automatic processing shall be:

---

[2] https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=2196553&SecMode=1&DocId=694350&Usage=2

[3] http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=108&CM=8&DF=&CL=ENG

[4] http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=&CL=ENG

obtained and processed fairly and lawfully;" and "stored for specified and legitimate purposes and not used in a way incompatible with those purposes", in practice, law enforcement agencies relied heavily on the provisions of Art. 9.2 of Convention 108 which states that derogations from Art. 5, 6 and 7 "shall be allowed when such derogation is provided for by the law of the Party and constitutes a necessary measure in a democratic society in the interests of protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences". At that time (some would say even now) there was little if any evidence of many police forces around Europe being allergic to collecting and processing personal data "just in case it comes in handy" without any specific reason or clear specific purpose.

The deliberations of the CJ-PD were finally encapsulated in R(87)15 and firstly through an innovation in the definitions section of that seminal Recommendation: "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." This definition therefore puts meat on the skeleton provided by Articles 5 and 9 of Convention 108 and was then further supplemented by the provisions of R(87)15's Article 2 where one reads:

> "2.1. The collection of personal data for police purposes should be limited to such as is necessary for the prevention of a real danger or the suppression of a specific criminal offence. Any exception to this provision should be the subject of specific national legislation."

This provision was the result of a two-year long debate within the CJ-PD and, in legal jargon, may also be interpreted as a "for the avoidance of doubt" provision." Building upon the words of Art 9 of Convention 108 and specifically "a necessary measure" and "is provided for by law" it laid down the principle that the police are no exception to the principle of purpose and that collection of personal data is limited to that which is strictly necessary "for the prevention of a real danger or the subject of specific criminal offence", thus placing firmly out of bounds the collection of personal data "just in case it comes in handy". Much to the chagrin of some national delegations (and notably those of Ireland and the UK which, respectively entered a general reservation and reservations to Arts 2.2 and 2.4 of R(87)15), this Recommendation left no doubt that legislative intervention was and remains required. If any European politician, government minister or lawmaker wishes to exempt a police force from the obligation to collect only that personal data which is necessary for the prevention of a real danger and the suppression of a specific criminal offence then he or she must take the trouble to reflect properly, indulge in an open and proper debate as a prerequisite to legislating specifically on the matter. When faced with the practical and political consequences of making such a choice, many politicians and law-makers often shy away from making any laws which may draw adverse public reaction on account of their being perceived as giving powers to the police which may be considered to be too intrusive.

This then was the context for R(87)15 at a time when the cold war was not yet over and the spectre of a state-sponsored Big Brother was still very much at the root of the reasoning behind this then-new legal instrument. Times have changed however. Originally (e.g. in 1984-1987 at the time of drafting of R(87)15) personal data used by the police was largely if not almost exclusively data collected "for police purposes". Today, in 2012-2013, there has been a shift to a position where police increasingly access data originally not collected by themselves but which would have been collected by other public agencies or very often a private entity (e.g. airline, bank, insurance company, transport company as in metro, bus, train, tram, taxi, etc.). This is a paradigm shift for police use of personal data. A law enforcement agency is today sometimes less concerned with the use of personal data that it itself collects for police purposes but rather is very interested in the personal data collected by third parties in the private sector - it should be said at the expense of the private sector - and which is normally collected for other purposes i.e. not for police purposes as defined by R(87)15. The situation envisaged in the brief's scenario as outlined in section 2

above is that of personal data collected in the private sector and then transmitted within the private sector or to law enforcement agencies, locally or across national boundaries. This was not the primary preoccupation of the authors of R(87)15 when dealing with communication of personal data when in Section 5.4 it is provided that "Communication of data to foreign authorities should be restricted to police bodies. It should only be permissible:

a. if there exists a clear legal provision under national or international law,
b. in the absence of such a provision, if the communication is necessary for the prevention of a serious and imminent danger or is necessary for the suppression of a serious criminal offence under ordinary law, and provided that domestic regulations for the protection of the person are not prejudiced."

This provision on international communication should be read together with Art 5.3 I of R(87)15. This states that the "communication of data to private parties should only be permissible if, in a particular case, there exists a clear legal obligation or authorisation, or with the authorisation of the supervisory authority." This provision is in turn complemented by Art 5.3.ii. which stipulates that "Communication to private parties is exceptionally permissible if, in a particular case: a. the communication is undoubtedly in the interest of the data subject and either the data subject has consented or circumstances are such as to allow a clear presumption of such consent, or if b. the communication is necessary so as to prevent a serious and imminent danger."

The authors of R(87)15 had contemplated file-matching and on-line access as may be seen in provisions of Art 5.6.: "The interconnection of files with files held for different purposes is subject to either of the following conditions:

a. the grant of an authorisation by the supervisory body for the purposes of an inquiry into a particular offence, or
b. in compliance with a clear legal provision.

Direct access/on-line access to a file should only be allowed if it is in accordance with domestic legislation which should take account of Principles 3 to 6 of this recommendation."

So while Principle 5 - Communication of data, is one of the longest sections of Rec (87)15, there one only finds provisions largely written with the communication of data collected by the police in mind. This is clear from the opening paragraphs on the scope of this Recommendation ("The principles contained in this recommendation apply to the collection, storage, use and communication of personal data for police purposes which are the subject of automatic processing") which should in turn be read together with the definition of police purposes outlined earlier.

In summary the most important European legal instrument dealing with data protection in the law enforcement sector regulates communication of data collected for police purposes to other police bodies and to private parties but,

i) not from private parties to the police, and
ii) not between private parties.

This means it does not regulate the two important instances envisaged in the scenario outlined in the brief which, in default of anything specific laid down by R(87)15, must then presumably fall under the general tenets of data protection law.

This consideration, therefore, takes one back to the principles of Convention 108 and specifically to its Art 12 which provides that:

> "The following provisions shall apply to the transfer across national borders, by whatever medium, of personal data undergoing automatic processing or collected with a view to their being automatically processed.
>
> A Party shall not, for the sole purpose of the protection of privacy, prohibit or subject to special authorisation transborder flows of personal data going to the territory of another Party.
>
> Nevertheless, each Party shall be entitled to derogate from the provisions of paragraph 2:
>
> insofar as its legislation includes specific regulations for certain categories of personal data or of automated personal data files, because of the nature of those data or those files, except where the regulations of the other Party provide an equivalent protection;
>
> when the transfer is made from its territory to the territory of a non-Contracting State through the intermediary of the territory of another Party, in order to avoid such transfers resulting in circumvention of the legislation of the Party referred to at the beginning of this paragraph."

The logic of the Convention and its drafters was the creation of a common European area where the same minimum standards of data protection applied equally regardless of geographic location and, therefore, the mere fact that personal data crosses a national boundary does not warrant the introduction of any additional safeguards or the creation of obstacles to such transborder data flow provided that the data flow is between parties to Convention 108.

It should be noted at this stage that while Convention 108 does not preclude its application to activities carried out by SIS, the drafting of Rec(87)15 was carried out with LEAs in mind and not SIS. In 1984-1987 there was no world-wide-web nor the petabytes of personal data generated by WWW every day across the Internet. It was still a world where on-line activities by private citizens had not yet come to the fore or indeed were in any way a significant part of everyday life. SIS were still working in a cold-war context, with an iron-curtain across Europe and not in the borderless cyber eco-system inhabited by over two billion of the world's population in 2013. It made sense then to keep rules for SIS and LEAs separate and an attempt to impose explicit and detailed data protection laws on SIS too would in 1987 have been seen as being a bridge too far.

Nor were there multinational corporations like Google, Facebook, Yahoo, Twitter and others all controlling huge data processing capabilities replete with personal data obtained by profiling every form of on-line activity possible in the Internet environment of 2013. The question that will later arise is whether this existing legal model is appropriate for modern-day circumstances where personal data flows across borders in daily torrents and is constantly being analysed and shared across borders by for-profit corporations, organized crime, LEAs and SIS. Is the old way, i.e. separate legal regimes, an adequate legal response to the de facto situation in 2013 where it is the same personal data generated by the same private citizens through the same transactions using the same browsers and search engines over the same ISPs and other service providers that is collected and analysed by for-profit corporations, organised crime, LEAs and especially SIS?

6 The brief's "scenario", Convention 108's Six-point test & 2002/58/EC

At this stage it is important to consider whether the scenario given in the brief is specific enough and contains all the details necessary to enable a clear answer to be given:

> "The paper may be based on a scenario where a private sector entity in country A disposes of information (threat intelligence on IP addresses, malware found, geo-location data) on multiple computer systems infected by malware and forming part of a botnet in country B (and other countries). The entity in country A shares this information with an ISP in country B who then contacts its customers to help them clean their systems. Alternatively, the entity in country A may share this information with a CERT or similar in country B who contacts owners of the infected systems."

It is noted that in the brief a number of key indicators are missing. The most important is that there is no indication as to whether country A or country B are parties to Convention 108. The second most important indicator which is missing is whether either country A or country B have laws which specifically govern or permit the flow of data within or from the private sector in circumstances where the communication of such data would prevent harm to innocent data subjects. The third most important indicator which is missing is whether country A or country B or both are member states of the European Union since this too could be a determining factor in establishing which legal regime would apply to the case in the scenario proposed.

It is convenient to start this part of the discussion by carrying out an analysis in terms of Convention 108 since this represents common ground between those European countries which are EU member states and those which are not i.e. all 28 EU member states are also party to Convention 108.

6.1 Convention 108

In the circumstances envisaged by the scenario given in the brief insofar as Convention 108 is concerned there are six important considerations to be made:

- Question 1: to what extent, if any, can the information referred to in the brief (threat intelligence on IP addresses, malware found, geo-location data) be considered to be personal data?

- Question 2: is the country from where the data originates a party to Convention 108?

- Question 3: does the country where the data originates have a law which explicitly provides that data collected for one purpose may be transmitted inside or outside the country for another purpose where such transfer of data constitutes a necessary measure in a democratic society in the interests of protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences; or protecting the data subject or the rights and freedoms of others?

- Question 4: is the country to which the data is transferred a party to Convention 108?

- Question 5: does the country to which the data is transferred have a law which explicitly provides that data collected for one purpose may be transmitted inside or outside the country for another purpose where such transfer of data constitutes a necessary

measure in a democratic society in the interests of protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences; or protecting the data subject or the rights and freedoms of others?

- Question 6: does the law of the receiving country provide equivalent protection to the law of the sending country?

The answers to the above questions therefore may depend on a number of variables – see Section 7 below - but the results in practice would not be dissimilar. In terms of Convention 108, if the answers to the six questions above are all Yes, then there is no legal obstacle (from a data protection point of view) to the transfer of personal data contemplated in the vignette scenario. If they are not all YES then the approach may be made quite algorithmic:

- The answer to question 1 above

If the answer to the first question is a NO i.e., the data is not capable of being linked to an identified or identifiable individual, then it lies outside the scope of data protection law.

- The answer to question 2 above

This question is asked here more for purposes of maximizing clarity rather than its impact on the overall answer. Put simply whether or not the country of the provider (Country A) has a data protection law or not is only relevant if it is compelled by its own domestic law to impose conditions on the transfer of the data. The onus of responsibility for the "onward processing" lies with the CERT or ISP in country B which by definition are normally outside the jurisdiction of Country A but are within the jurisdiction of country B. It would be extremely rare for a transferor in country A to deliberately expose themselves to culpability standards in Country B and it is far more likely to be the transferee which would sometimes accept the onus of certain conditions imposed by the transferor. If the country where the data originates is not a party to Convention 108, has no restrictions on transfer of personal data held by the private sector and wishes to transfer such data to a public sector or private sector entity within Europe then the same considerations kick in and it is the law of the receiving country which is in practice most relevant. Does the country where the data is received have a law which explicitly provides that data collected for one purpose may be transmitted inside or outside the country for another purpose where such transfer of data constitutes a necessary measure in a democratic society in the interests of protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences; or protecting the data subject or the rights and freedoms of others? If the answer is Yes, then there should be no problem to use the data for a purpose which is explicitly provided for by law since it benefits the data subject and prevents him or her from harm.

- The answer to question 3 above

This is more relevant where country A is an EU member state and especially a non-EU CoE member state since it is, in terms of Art 9 of Convention 108 bound to have a specific provision at law which expressly authorizes that data collected for one purpose may be transmitted inside or outside the country for another purpose where such transfer of data constitutes a necessary measure in a democratic society in the interests of protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences; or protecting the data subject or the rights and freedoms of others? If the answer is Yes, then there should be no problem to use the data for a purpose which is explicitly provided for by law since it benefits the data subject and prevents him or her from harm. This question therefore is important to

determine the legality of the data transfer where the originating state is either an EU member state or a non EU CoE member state.

- The answer to question 4 above

If the answer to the second and fourth questions above is a YES but the answer to the third question – and possibly the fifth question above is a NO i.e. that either or both countries do not have specific legal provisions which permit the transfer of such data for the purpose of preventing harm to a data subject, then the situation is possibly one of illegality but where the solution is relatively simple: enact the required legislation, something which should not require undue time and effort. This would not be an unusual situation inside Europe. Many European countries, both EU and non-EU member states, possibly find themselves in a position where they do not have specific laws with provisions aimed at specifically regulating the flow of personal data. If, on the other hand the answer to question 4 is a NO then one needs to go to question 6 in search of a YES answer to that question.

- The answer to question 5 above

As in the case of the answer to question 3 this is important to determine the legality of the data transfer in those states which are parties to Convention 108

- The answer to question 6 above

If the answer to the second and third question above is a YES and the answer to the fourth question above is a NO then the situation becomes more difficult since the export of the personal data would not be permissible on grounds of possible lack of equivalent protection in the receiving state something which can be determined and/or resolved on an ad hoc through measures such as the Safe Harbor Agreement or Binding Corporate Rules.

6.2 Directive 2002/58/EC

It is submitted that the questions asked in the scenario acquire a special dimension if either or both country A or country B are EU member states since in that case they are bound by Directive 2002/58/EC on privacy and telecommunication networks, which in turn relies on definitions also to be found in Directive 2002/21/EC. The definitions found in these two Directives and the provisions of Art 4 of 2002/58/EC are very relevant to the scenario:

> Article 4
> Security
> 1. The provider of a publicly available electronic communications service must take appropriate technical and organisational measures to safeguard security of its services, if necessary in conjunction with the provider of the public communications network with respect to network security. Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented.
> 2. In case of a particular risk of a breach of the security of the network, the provider of a publicly available electronic communications service must inform the subscribers concerning such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, of any possible remedies, including an indication of the likely costs involved.

It seems clear that Article 4 of 2002/58/EC actually imposes on the service provider a duty of informing subscribers concerning "risk of breach of security of a network" and this in addition to

unspecified "appropriate technical and organizational measures" which may conceivably also include notification of a CERT or other service providers or end-users.

These appropriate technical and organizational measures could conceivably include a mutual assistance agreement with other service providers whether within or outside national boundaries. Such a standing mutual assistance agreement would help overcome any perceived limitations of the wording of Art 4 where it speaks of "its services" as in the provider "must take appropriate technical and organizational measures to safeguard security of its services" and as in "its services" and not those services of another service provider.

The scenario speaks of "threat intelligence" which falls under the security remit and obligation imposed by Article 4 of 2002/58/EC and specifies, by way of example, "threat intelligence on IP addresses, malware found, geo-location data on multiple computer systems infected by malware and forming part of a botnet in country B". This would prima facie actually comprise a formal legal obligation which in data protection terms constitutes precisely that which is required by Article 9 of Convention 108, i.e. "is provided for by the law of the Party and constitutes a necessary measure in a democratic society in the interests of protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences, protecting the data subject or the rights and freedoms of others."

The creation of malware, botnets etc. is a criminal offence in terms of the Cybercrime Convention (Convention 185) so there can be no question of breaching data protection law if a service provider advises another service provider or a CERT in another country and provides them related threat intelligence. This would constitute a reasonable security measure and is actually discharge of a duty, an obligation at law to provide reasonable security measures.

7 The questions set in the brief: a point-by-point response

Sections 5 and 6 above establish three important points amongst others:

i. that in the scenario envisaged in the brief, the data is primarily collected for network security purposes and thus not for police purposes as defined by R(87)15. In other words, the scenario therefore falls largely outside the remit of R(87)15 and that in order to answer the questions set, one cannot properly rely on R(87)15 and one should instead rely on more generic data protection law starting with Convention 108;

ii. that even if one were to argue that such data has police purposes conferred upon it *ex post* by virtue of, say, the EU's 2006 Data Retention Directive[5], or by virtue of the widest interpretation possible of what "constitutes a necessary measure in a democratic society etc." and that the scenario falls under R(87)15, the latter still lacks sufficiently detailed regulations governing the collection and transmission of data by a private entry to another private entity or even the police so one still needs to largely ignore R(87)15's provisions and instead seek guidance elsewhere, either in Convention 108 or in Directive 95/46/EC (Data Protection) or else Directive 2002/58/EC;

5 The Data Retention Directive relies completely on the logic of suppression of criminal offences and public safety in order to justify it existence as may be seen from para 4 of the recitals :

4) Article 15(1) of Directive 2002/58/EC sets out the conditions under which Member States may restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of that Directive. Any such restrictions must be necessary, appropriate and proportionate within a democratic society for specific public order purposes, i.e. to safeguard national security (i.e. State security), defence, public security or the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communications systems."

iii. That the question is largely a non-issue in the cases where Country A is a member of the European Union since in that case the passing on of threat intelligence is not in breach of data protection law but actually discharges a legal duty to provide security in electronic communication systems and this in terms of Directive 2002/58/EC.

The merits of an algorithmic approach when analyzing the case premised in the scenario will be defined further in the conclusions but at this stage it is useful to systematically go through the questions set in the brief. If taken one by one, and in the light of the background given above, the answers to the questions set out in the brief may be set out as follows.

7.1 Which data protection laws apply?

Which data protection laws apply to the delivery of the information: the legislation of the provider of the information (country A), or the legislation of the receiver of the information (assuming here that both the entity receiving the information and the owner of the infected device are in country B)?

Before embarking on the answer to this question, it is worth reflecting on the generic effect of Convention 108 on location of the parties. It is here that Article 1 of Convention 108 is particularly instructive:

> "The purpose of this convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection").

This opening provision immediately puts certain elements of the case in stark perspective: the intention of the legislator is clear in that the location of the individual as expressed in the terms "whatever his nationality or residence" is irrelevant. The minimum standards of protection must be assured wherever one is found within territories falling under the jurisdiction of parties to the convention. In communicating such data to Country B, Country A is carrying out an action which is justifiable in terms of data protection law and specifically Art 9 of Convention 108 since it protects the data subject and is an attempt to mitigate or suppress a criminal offence. Art 9, furthermore requires that such an action is provided for by law, something which is (or should be) already a given in all 28 EU member states which are bound by Art 4 of 2002/58/EC. For the other nineteen member states of the Council of Europe which are not EU member states as well as for other non-European states "provided for by law" is therefore a requirement which would need to be verified and established on a case-by-case basis.

All this being said, certain basic tenets of law need to be borne in mind. The data controllers in Country A and Country B both need to and can reasonably be expected to respect the data protection laws and other applicable laws in their own respective countries. Various permutations may be briefly examined in order to determine where a problem may actually lie. Some of the main permutations may be summarized as in the following table:

	Permutation/Variable	Problem?	Reason	Condition
1	Where Country A and Country B are EU member states	No problem	Scenario covered by Art 4 of 2002/58/EC2	
2	Where Country A is an EU member state and Country B is non-EU but is a CoE 108 MS	No problem	Scenario covered by Art 4 of 2002/58/EC for A and covered by Art 9 Convention 108 for both A and B	
3	Where Country A and Country B are both CoE 108 member states but not EU MS	No problem	Scenario covered by Art 9 Convention 108	Provided that there is a specific law which permits communication of data "to protect data subject and/or suppress a criminal offence"
4	Where Country A is neither EU member state nor party to Convention 108 but Country B is an EU member state	No problem	Country B is covered by Art 4 2002/58/MS and Art 9 Convention 108	Provided that there is a specific law which permits communication of data "to protect data subject and/or suppress a criminal offence"
5	Where Country A is neither EU member state nor party to Convention 108 but Country B is a Coe 108 member state	No problem	Country B is covered by Art 9 Convention 108	Provided that there is a specific law which permits communication of data "to protect data subject and/or suppress a criminal offence"
6	Where Country A is either EU member state or party to Convention 108 but Country B is neither EU member state nor CoE	Problem	Country A cannot transfer the data to Country B unless adequate protection is afforded to data	If not covered by CoE or EU adequacy procedure then BCR or other adequate safeguard needed

It is submitted that in each of the cases in permutations 1-5 above, the law of both countries applies but that this in practice should not create any serious problems since they are operating in an area of law which is harmonized by either Convention 108 or 95/46/EC or both. A problem only really arises in the case of permutation 6 above where the receiving country is not operating within an environment which is harmonized with a standardized European data protection regime and where therefore ad hoc bilateral measures (such as Binding Corporate Rules) may be deployed in order to protect the rights of the data subject to a level deemed to be adequate at European standards.

7.2 If the law of the country of the infected device applies, why and how?

If the law of the country of the infected device applies (country B), does it apply for the simple fact that the information is related to a person that can be identified in this country? Or will the law of the receiving country apply only in certain circumstances (for instance, when the provider of the information who is based in country A proactively establishes a connection to the infected device in country B)?

The way this question is framed may be misleading. It is not the connection to an infected device that invokes data protection law but the control, use and transfer of personal data. The law of country B applies once a data controller in that country processes it. It is the location of the controller that determines the law which is applicable. Since Convention 108 grants protection to any citizen "regardless of his nationality or place of residence" a data subject has a full range of rights over his/her personal data wherever it may be found within the EU or within a member state of Convention 108 even if he or she is not resident in the same country where the data controller if established. Thus, if an infected device is in country B, it is irrelevant if the person connected to that device is actually in country B or C or D. He or she has the same rights and merits the same level of protection.

7.3 Which entity is supposed to comply with the data protection law of the receiving country?

Which entity is supposed to comply with the data protection law of the receiving country: the provider of the information (which is based in country A) or the receiver of the information (the ISP or the CERT based in country B)?

The provider of the information is expected to abide by the laws of the country where he is established (country A in this instance) while the receiver of the information located in Country B is expected to comply with the law in country B. The Table given above suggests that in most cases, the situation between European countries should, in theory, be harmonized to an extent where it makes little difference as to which country's law is actually applied since they are all supposed to provide a minimum level of protection to the data subject and similar levels of rights and responsibilities for data controllers. In the case of permutation 6 the problem is not supposed to arise since the level of protection afforded must be adequate. The issue only really arises in the case of Permutation No 4 and/or Permutation No 5. What happens if, say, an entity in the USA wishes to export personal data with threat intelligence to Europe? In that case, the minute the data comes under the control of a data controller under European jurisdiction (EU or non-EU so long as minimum Convention 108) then it is subject to the full breadth of the applicable European law as deployed on the territory where the data controller is established (Country B). The provider of the information (in this case where the USA is country A) is bound to comply with the laws of Country B only if he/she is still effectively a data controller of data located within the jurisdiction of country B. Otherwise, if a transfer of data has been effected then it is the transferee in country B who is responsible.

7.4 If the information is delivered to country B for removal of malware, what obligations for the provider in country A?

If the information is delivered to country B for the exclusive purpose of helping to remove malware, is the provider (based in country A) of the information exempted from some or all obligations pursuant to data protection law of the receiving country (country B)?

In practice (or at least in logic) the question should not even arise. The provider (based in country A) is presumably outside the jurisdiction of Country B and has delivered the information to a data controller or intermediary in Country B who is then effective controller of the data and falls under the jurisdiction of country B. It is the transferee and not the transferor who is now responsible for full compliance with the data protection laws of country B.

7.5 If the information is delivered to country B for criminal investigations, what obligations for the provider in country A?

If the information is delivered for the purpose of supporting criminal investigations, is the provider (based in country A) of the information exempted from some or all obligations pursuant to data protection law of the receiving country (country B)?

In this case, all the preceding answers should be read together. Following the logic expounded above it makes little difference what the purpose of the communication of the data is i.e. either network security or support of criminal investigations. The provider (the transferor) is generally subject to the laws of country A and the recipient or transferee is generally subject to the laws of country B. Once the data arrives in country B its further processing falls subject to the law of country B but it is generally the transferee (e.g. the ISP or the CERT) who is expected to ensure compliance with the law of that country and not the transferor who is generally beyond the reach of country B.

8 Impact of January 2012 draft proposals by European Commission

Like so many other scholars and analysts, the author of this report has spent the best part of twenty-two months observing the ups and downs of the so-called Data Protection Reform Package (DPRP)[6] put together over many years of preparation by the European Commission (EC). The precise current and future impact of the draft proposals by the European Commission is hard to gauge with any degree of accuracy at the time of submission of this study at end September 2013, especially since it is not yet certain what the final form of the DPRP will be like or whether there will be any DPRP agreed at all by the time the European Parliament is dissolved in May 2014 . Moreover it is difficult to avoid the impression that the DPRP may in some instances at least have been overtaken by events and especially the fall-out of the Snowden affair which broke in May 2013.

Some time between the end of November and early December 2011 the inter-service consultation draft version of the DPRP was leaked[7] in time for many academics, corporate counsel and lobbyists to use the Christmas vacation period to pore over the details. Only to eventually learn 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.[8]

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. Rather than following the logic of one comprehensive legislative package pegged at Regulation level 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 (e.g. 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

6 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) */

7 Statewatch, "Observatory on Data Protection in the EU" (2012), available at http://www.statewatch.org/eu-dp.htm

8 "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

> "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 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."[9]

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"[10] of the first four chapters of the Regulation.

The way in which the DPRP and especially the draft Directive may sit with and occasionally within the Council of Europe's framework of legal instruments providing safeguards for data protection in the police and law enforcement agency (LEA) and Security and Intelligence Services (SIS) sectors is discussed in some detail in a separate report[11] by the present author submitted to the Council of Europe contemporaneously with this study. That study on the same recommendation R(87)15 which has also been referred to in many instances in the foregoing analysis in this present report finds that "by and large the Recommendation has been widely adopted across Europe to an extent that many European states prima facie already regulate police use of personal data in a way comparable but not necessarily identical to that envisaged in the current draft of the European Commission's proposal 25.1.2012 COM(2012) 10 final 2012/0010 (COD) 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". This general finding in no way obviates the need for urgent action on this sector." [12] The same study on Rec(87)15 "identifies two overall findings and thirty-one provision-specific findings in relation to the provisions of R(87)15 and places these in the context of eight realities as at September 2013.

In response to the overall findings of disparity of provisions and lack of harmonisation, the Report advocates that the time has come for a binding legal instrument which is capable of being deployed across sectors which have hitherto often been parallel worlds: that of law enforcement agencies (LEAs) and the other of Security & Intelligence Agencies (SIS).

The Report takes into account the available evidence of utility of the EU's 2006 Data Retention Directive as well as the significance of the Snowden revelations for privacy & data protection. These considerations reinforce the Report's recommendations that the Council of Europe offers the right forum for one or more of at least three options which could produce a suitable new binding legal instrument:

---

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

10 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

11 Cannataci Joseph A & Caruana Mireille M., "Recommendation R (87) 15 – Twenty–five years down the line" a report submitted to the Council of Europe on 26 September 2013.

12 Ibid. at page 2

- (1) an entirely new multi-lateral treaty or Convention which would contain mandatory provisions applicable to the LEA and SIS handling of personal data;
- (2) an additional protocol to the CoE's Data Protection Convention (ETS 108) encapsulating the provisions envisaged in Option 1 and/or
- (3) an additional protocol to the CoE's Cybercrime Convention (ETS 185) incorporating some of the provisions envisaged in Options 1 and 2.

The Report finds that the urgency for and the onus upon the Council of Europe to take immediate action to produce a new binding instrument is compounded by the Snowden revelations and the possible inadequacy of EU responses in the sphere of national security on account of exclusions of competence by Art 4 Section 2 of the EU Treaty". The separate study concludes that "it would be worse than useless to rely on the legal instruments currently in place or presently contemplated, as one would be relying on the illusion that the current and contemplated legal instruments provide an adequate response to the realities of 2012-2013 when they patently do not. They provide a basis for further and on-going development of the regulatory framework but not for reliance upon it in its present form."[13]

Against this background, it should be abundantly clear to any analyst or policy maker that the right formula to tackle the LEA/SIS conundrum will be hard to develop and more complicated still for those 28 member states of the Council of Europe which also happen to be members of the EU. Firstly there appears to be disagreement between the EU member states as to which type of legal instrument – never mind the content – is actually the best vehicle for the DPRP.

> "The Presidency notes that eight Member States (Belgium, the Czech Republic, Denmark, Estonia, Hungary, Sweden, Slovenia and the UK) still do not support the Commission's choice to use a regulation as the legislative instrument in this process, and would prefer that the current EU Data Protection Directive 95/46/EC ("Data Protection Directive") be repealed and replaced by another directive. The Presidency's amendments leave flexibility for the Proposed Regulation to be transformed into a directive in future. The Presidency has therefore not ruled out the possibility of using a different instrument."[14]

As if this level of disagreement about the right type of instrument to adopt at EU level were not enough, the problem for EU policy-makers complicates itself further when taking into account certain legal constraints which currently exist within the EU but not in the Council of Europe. The group of 28 EU member states are at present faced with a number of procedural difficulties and political uncertainties should they wish to go it alone in the immediate future. The type of surveillance carried out in those sectors revealed by Snowden crosses over between strictly LEA areas of competence such as serious organised crime and into national security, an area which in terms of Article 4 Section 2 of the Treaty of the European Union falls outside the scope of EU law: "In particular, national security remains the sole responsibility of each Member State."[15]. It is reported personally to the author by reliable sources who must at the time of writing remain unnamed that this provision has already been utilised by the UK and Sweden to block some level of formal action at EU level over the Snowden affair. This in spite of the fact that a special ad hoc working group including the data protection commissioners from Austria and Slovenia[16] has been

13 Ibid.

14 www.huntonprivacyblog.com/2013/06/articles/council-of-the-european-union-releases-draft-compromise-text-on-the-proposed-eu-data-protection-regulation/ last accessed on 30 September 2013

15 Art 4 Section 2, Consolidated version of the Treaty on European Union, Official Journal of the European Union.

16 The Information Commissioner Nataša Pirc Musar has been appointed member of a special ad hoc working group EU – USA.

Accessed at https://www.ip-rs.si/index.php?id=272&tx_ttnews[tt_news]=1182&cHash=a8790b0646e9527bd35eb55e1a2f052f

appointed with a mandate "to clarify the actual state of activities of the US National Security Agency (NSA) in relation to the alleged collection of information and personal data on EU citizens".[17]

There is not much transparency or information forthcoming about the results of joint EU-USA negotiations on this matter at this stage: "The group is not allowed to make any public statements before the end of the mandate, when a report needs to be submitted to the European Commission"[18] Other reports held that: "The EU members of the group will report to Member States' ambassadors to the EU in October. Their conclusions will be shared with the EEAS, the European Commission, and the Council's secretariat, but, officials said, it is not clear if the institutions will receive the report itself. No official was able to say if any of the conclusions would be shared with the public. A national diplomat said that the Member States were showing little enthusiasm for pursuing their inquiries at the EU level."[19]

Thus, while there has been considerable noise made about the Snowden revelations in the European Parliament,[20] especially during September 2013,[21] it is unlikely that the European Council would move away from a position where at least one national EU Government, possibly more, are opposed to concerted action on this issue at EU level. The agenda for the European Council scheduled for 25 October 2013 and published on 23 September 2013 makes no specific mention of any discussion of reports resulting from the Snowden allegations though this can possibly be included under the standard catch-all "The European Council may also address specific external relations issues in the light of developments on the international scene."[22]

Would the same apparent lack of enthusiasm remain evident at Council level in the period October – December 2013? Would the wider ambit and track-record of the Council of Europe provide an environment where the lack of enthusiasm of one or even a handful of national governments would not prevent the creation of an impetus which would result in new legally enforceable safeguards? Would an overwhelming majority in say the T-PD or the T-CY leave a tiny minority – or even a minority of one – quite hopelessly isolated in their opposition to concerted European and eventually international action? These are some of the questions which remain outstanding at the time of finalisation of this version of this report. It should be noted too that matters for the EU States are not helped by the uncertainty that hangs over the fate of the draft Directive[23] aiming at data protection in the criminal justice sector. While some data protection experts welcome the draft Directive as a step forward in terms of EU law where it represents an improvement over the currently applicable EU law CFD/977/JHA/2008, at the time of writing it is uncertain whether it will be adopted at all before the EU parliament is dissolved in May 2014 or which is the precise form it would go through in.

17 Ibid.

18 Ibid.

19 Gardner, Andrew. 2013. EU and US to discuss snooping allegations. The European Voice. Accessed at http://www.europeanvoice.com/article/imported/eu-and-us-to-discuss-snooping-allegations/77956.aspx

20 Schmitz, Gregor-Peter. 2013. EU Parliament Furious about NSA Bank Spying. Der Spiegel. Accessed at http://www.spiegel.de/international/europe/nsa-spying-european-parliamentarians-call-for-swift-suspension-a-922920-druck.html

21 Belgacom Attack: Britain's GCHQ Hacked Belgian Telecoms Firm. Der Spiegel 20 September 2013. Accessed at http://www.spiegel.de/international/europe/british-spy-agency-gchq-hacked-belgian-telecoms-firm-a-923406.html

22 European Council (24-25 October 2013) – Annotated draft agenda – Doc 12389/13. Accessed at http://www.european-council.europa.eu/council-meetings/documents-submitted-to-the-european-council?lang=en

23 European Commission's proposal 25.1.2012 COM(2012) 10 final 2012/0010 (COD) 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, http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_10_en.pdf

In real terms, however, its adoption, or lack of it, would have little real impact for European citizens. Firstly, as demonstrated by the results of the research in the PUPIE project[24], most of the provisions contemplated in this draft Directive have already in point of fact been transposed into national law across most EU states and indeed many states in Europe thanks to the impact of R(87)15. Secondly, even if the current or a revised draft of the proposed European Directive were to see the light of day, it would not adequately address the data protection implications raised by Snowden's revelations, since 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. If the Draft DPRP does make it through in its current form, however, there is no available evidence which would suggest any change of Recital 90 of the Regulation beyond the version published to date so the following analysis is the best response possible to that part of the brief which deals with Recital 90.

9 Recital 90 of the draft EU Regulation on data protection

The current Recital 90 of the draft Regulation to which the brief for this study makes direct reference appears to be a rather forlorn result of the general watering down of the Regulation's principles which took place some time between the 29th November 2011 and the 25th January 2012. This Recital 90 does not appear to have yet been targeted for explicit change according to the latest compromise texts released by the European Commission[25] and the Irish Presidency in May-June 2013.

Approximately the first half of the text of the current draft Recital 90 seems to have been lifted verbatim from the previous draft Recital 74 which on the 29 Nov 2011 read as follows:

> (74) Mutual assistance treaties or international agreements between third countries and the Union or a Member State may provide for the exchange of personal data under specific circumstances, for specific purposes and with appropriate safeguards for the data subjects. However, some third countries enact laws, regulations and other legislative instruments which purport to directly regulate data processing activities of natural and legal persons under the jurisdiction of the Member States of the Union.
>
> The extraterritorial application of these laws, regulations and other legislative instruments may be in breach of international law and may impede the attainment of the protection of individuals guaranteed in the Union by this Regulation.
>
> Consequently, provision should be made to prohibit a controller or processor to directly disclose personal data to requesting third countries, unless authorised to do so by a supervisory authority.

The original intent behind the then Recital 74 was most likely to give the reasons for the raison d'etre of the draft Article 42 which appeared in the draft Regulation leaked before Christmas 2011[26] and which is reproduced below for reference:

---

24 Cannataci Joseph A & Caruana Mireille M., "Recommendation R (87) 15 – Twenty–five years down the line" a report submitted to the Council of Europe on 26 September 2013 already cited supra.

25 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

26 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) Version 56

(29/11/2011) last accessed on 24 Sep 2013 at http://www.statewatch.org/news/2011/dec/eu-com-draft-dp-reg-inter-service-consultation.pdf

Article 42

Disclosures not authorized by Union law

1. No judgment of a court or tribunal and no decision of an administrative authority of a third country requiring a controller or processor to disclose personal data shall be recognized or be enforceable in any manner, without prejudice to a mutual assistance treaty or an international agreement in force between the requesting third country and the Union or a Member State.
2. Where a judgment of a court or tribunal or a decision of an administrative authority of a third country requests a controller or processor to disclose personal data, the controller or processor and, if any, the controller's representative, shall notify the supervisory authority of the request without undue delay and must obtain prior authorisation for the transfer by the supervisory authority in accordance with point (b) of Article 31(1).
3. The supervisory authority shall assess the compliance of the requested disclosure with the Regulation and in particular whether the disclosure is necessary and legally required in accordance with points (d) and (e) of paragraph 1 and paragraph 5 of Article 41
4. The supervisory authority shall inform the competent national authority of the request. The controller or processor shall also inform the data subject of the request and of the authorisation by the supervisory authority.
5. The Commission may lay down the standard format of the notifications to the supervisory authority referred to in paragraph 2 and the information of the data subject referred to in paragraph 4 as well as the procedures applicable to the notification and information. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

It might well be argued that this draft Art 42 as proposed before December 2011 was at least partially designed to provide a legal defence to European-based controllers of personal data who may have been served a request to transfer personal data in terms of the law of a non-EU state such as the United States and who would deem such a request not to be in compliance with the Regulation even if there existed a bilateral agreement or a basis in national law of that particular EU state enabling the transfer of data to another non-EU state. As has also been noted in some of the very first pieces of published analysis[27], by 25 January 2012 the relatively strict and explicit safeguards of the draft Art 42 had disappeared with the only appropriate conclusion to be derived from such an omission being that the legislator no longer intended the Regulation to provide such safeguards.

Instead the attentive reader, would have noted that by 25 January 2012 Recital 74 lost the explicit reference to

> "Mutual assistance treaties or international agreements between third countries and the Union or a Member State may provide for the exchange of personal data under specific circumstances, for specific purposes and with appropriate safeguards for the data subjects"

and the bulk of its remaining text was renumbered as the first half of the new Recital 90, the effect of which is not immediately clear:

27 G Hornung, "A General Data Protection Regulation For Europe? Light And Shade In The Commission's Draft Of 25 January 2012", (2012) 9:1 SCRIPTed 64 http://script-ed.org/?p=406

> Recital 90
>
> "Some third countries enact laws, regulations and other legislative instruments which purport to directly regulate data processing activities of natural and legal persons under the jurisdiction of the Member States. The extraterritorial application of these laws, regulations and other legislative instruments may be in breach of international law and may impede the attainment of the protection of individuals guaranteed in the Union by this Regulation. .Transfers should only be allowed where the conditions of this Regulation for a transfer to third countries are met. This may inter alia be the case where the disclosure is necessary for an important ground of public interest recognized in Union law or in a Member State law to which the controller is subject. The conditions under which an important ground of public interest exists should be further specified by the Commission in a delegated act."

In order to best understand the possible real meaning of the new Recital 90 it is useful to dissect the other differences between the old Recital 74 and the new Recital 90. Gone is the intent to prohibit certain actions which may safeguard data subjects as previously carried forward in the previous Draft Art 42 which has since disappeared:

> Consequently, provision should be made to prohibit a controller or processor to directly disclose personal data to requesting third countries, unless authorised to do so by a supervisory authority.

Instead the new Recital 90 also gained the intriguing if rather obvious statement

> Transfers should only be allowed where the conditions of this Regulation for a transfer to third countries are met.

So basically if the Regulation elsewhere permits transfer of data to a third country – such as the US or other member of the Five Eye group e.g. in terms of a mutual assistance treaty founded upon the notion of national security or some other such grounds "in the public interest" this could not be refused on the strength of the Regulation as previously intended in the "disappeared" Art 42. Not content with the clear dilution which has resulted with the disappearance of the pre-Jan 2012 Art 42, the next insertion of new text in Recital 90 now sounds rather like a for the avoidance of doubt clause:

> This may inter alia be the case where the disclosure is necessary for an important ground of public interest recognized in Union law or in a Member State law to which the controller is subject

Once again, thanks to this post-Nov 2011 amendment, the status quo existing in 2012 is preserved. The new Regulation is not going to rock the boat in those cases where e.g. the UK may in terms of its own law authorize transfer of personal data to the United States for "an important ground of public interest" such as national security or economic interest.

So how is this recital to be interpreted? Well, according to the EU's Joint Practical Guide "10. The purpose of the recitals is to set out concise reasons for the chief provisions of the enacting terms, without reproducing or paraphrasing them. They shall not contain normative provisions or political exhortations"[28]. So if Art 42 was deleted from the draft precisely which articles is the Recital 90 setting out concrete reasons for? Given the dilution outlined above, most of the newer parts of

28 Joint Practical Guide Guide of the European Parliament, the Council and the Commission for persons involved in the drafting of legislation within the Community Institutions" Last accessed on 24 September 2013 at http://eur-lex.europa.eu/en/techleg/10.htm

Recital 90 would appear to exist to explain the raison d'etre of those provisions in the Regulation which retain the status quo or now make it easier to export personal data outside the EU.

The only rather half-hearted attempt at contemplating a safeguard is to be found in the concluding sentence of Recital 90:

> "The conditions under which an important ground of public interest exists should be further specified by the Commission in a delegated act."

In summary, the only reasonable conclusion that may be drawn about Recital 90 in the current draft of the Regulation is that the first half of Recital 90 i.e. that part which lives on from the old Recital 74 is little more than a smokescreen. The effective part of the Recital are the new parts indicated above with an effect which has been neatly summed up in the position paper of the EDRI:

> "The draft Regulation in its current version does not address the challenge of data transfers to third countries by virtue of extra-territorial laws, regulations and other legislative instruments, including for the purpose of law enforcement. It should be noted that existing practice in this area is very disquieting. Specific risks are related to the processing of data in cloud computing, when the providers of such services are legally established outside the EU. For example, under the U.S. Foreign Intelligence Surveillance Act of 2008 Act (Article 1881), the U.S. government is entitled to carry out surveillance of European data subjects on the basis of their data being processed by U.S. companies. The draft Regulation does not provide for any specific guarantees in this regard while, at the same time, aims at facilitating the transfer of personal data to third countries". [29]

10 Private-public data sharing in the post-Snowden era[30]

Most of the previous sections in this study and its recommendations were researched and written well before the revelations made about PRISM and similar programmes by Edward Snowden throughout the months since May 2013. It will be noted however that the bulk of the personal data that Snowden confirmed is being regularly processed by the NSA and GCHQ - to name but two of the intelligence agencies involved - is data collected and processed in the course of transactions by private citizens with other private citizens and/or commercial corporations in on-line media owned and operated by the private sector.

The issues for privacy and data protection of European citizens posed by programmes such as PRISM, TEMPORA and X-Keyscore have been dealt with in some detail elsewhere and most recently in a briefing note to the European Commission's Directorate General for Internal Policies.[31] Such studies should be read together, but not confused, with ongoing debates over the value of personal data processed "for police purposes" under the 2006 Data Retention Directive

29 Transfers to Third countries last accessed on 24 September 2013 at http://protectmydata.eu/topics/transfers-to-third-countries/

30 This section was added as part of an up-date exercise carried out between January and September 2013 and is in large part common to the section "Epilogue for the post-Snowden era" contained in the Report Recommendation R (87) 15 – Twenty–five years down the line by Professor Joseph A. Cannataci and Dr. Mireille M. Caruana submitted for consideration by the Council of Europe's Consultative Committee on Data Protection T-PD

31 Bowden, Caspar. The US National Security Agency (NSA) surveillance programmes (PRISM) and Foreign Intelligence Surveillance Act (FISA) activities and their impact on EU citizens' fundamental rights. A briefing note prepared for Directorate General for Internal Policies, Policy Department C: Citizens' Rights and Constitutional Affairs. Accessed at http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/briefingnote_/briefingnote_en.pdf

where the latest evidence made available in the public domain[32] is not as complete or as clear as one would wish. As one looks at all the various ways in which personal data is processed for use by LEAs and SIS one should remember that beyond PRISM and TEMPORA the personal data of European citizens is also being captured en masse in 28 of the 47 member States of the Council of Europe as a result of the EU's 2006 Data Retention Directive (DRD). There can be little doubt that the European Commission is trying its best to put together the available evidence on the basis of statistics provided by member States but it is careful to make no claims as to the conclusions that could be drawn from statements like "It appears that there are over two million requests per year for retained data, equivalent to about two requests for every police officer in the EU or 11 requests for every 100 recorded crimes".

Indeed when it comments on the quantitative data at its disposal it warns that "it would not be possible to identify meaningful statistical trends only a few years after the DRD entered into force." Some qualitative data recently published is however very valuable: thanks to the European Commission's latest report we obtain an insight into the way data retention proved useful or how its absence proved to be a hindrance. Summaries have been made available for five (5) cases in the category of terrorism, twenty-one (21) cases of murder and manslaughter, eleven (11) cases of Serious sexual offences and child abuse, nine (9) cases of buying or offering online child pornography, six (6) cases of Drugs trafficking, six (6) cases of armed robbery, twenty-four (24) cases of burglary, theft and organised trafficking, five (5) cases of cybercrime and six (6) cases of fraud. These latest revelations in a report released after March 2013 will doubtless fuel the debate further.

With the member states apparently unable to report a total of more than ninety-three (93) documented cases over what appears to be a period of some seven years since the Directive came into force on 03 May 2006[33], legitimate questions on the proportionality and cost-effectiveness of the DRD will doubtless be raised over the coming months and years. Yet citizens concerned with their privacy and data protection can take some solace that access to their personal data collected and processed under the DRD often (but not always in all countries) at least requires a court order[34]. That is a conventionally strong safeguard which is most often conspicuously missing in cases where their personal data being collected under PRISM, TEMPORA et al.

Indeed the situation in the United States appears to have become considerably worse than in Europe on at least two counts: duration of data retention and legal safeguards. Whereas the DRD makes it mandatory in the EU to retain traffic data for anything between six to twenty-four months, the latest revelations in the United States suggest that the NSA has the capability "to look back on the last 365 days' worth of DNI metadata seen by the Sigint collection system, regardless whether or not it was tasked for collection."[35] This in a context where "an internal briefing paper

32 See report: Evidence for necessity of data retention in the EU. Accessed at http://ec.europa.eu/dgs/home-affairs/pdf/policies/police_cooperation/evidence_en.pdf

33 The actual time-span over which the effectiveness of the DRD may be measured is in point of fact rather variable and is not uniform across Europe since the Directive entered into force in September 2007 for telecoms data with the option of delaying its coming into force until March 2009 for internet data, an option which most Member states decided to take up. Moreover in some states, most notably Germany, Romania and Czech Republic there were further delays in its implementation on account of a number of legal challenges in the courts right up to constitutional level.

34 This aspect is regulated by article 4 of the DRD which lays down that "Member States shall adopt measures to ensure that data retained in accordance with this Directive are provided only to the competent national authorities in specific cases and in accordance with national law. The procedures to be followed and the conditions to be fulfilled in order to gain access to retained data in accordance with necessity and proportionality requirements shall be defined by each Member State in its national law, subject to the

relevant provisions of European Union law or public international law, and in particular the ECHR as interpreted by the European Court of Human Rights."

35 JAMES RISEN and LAURA POITRAS, N.S.A. Gathers Data on Social Connections of U.S. Citizens, New York Times 28 September 2013 last accessed on 30 September 2013

from the N.S.A. Office of Legal Counsel showed that the agency was allowed to collect and retain raw traffic, which includes both metadata and content, about "U.S. persons" for up to five years online and for an additional 10 years offline for "historical searches."[36] The nature of legal safeguards in the USA for use of metadata appear to be scant "Much of the NSA's data collection is carried out under section 702 of the FISA Amendments Act. This provision allows for the collection of data without individual warrants of communications, where at least one end of the conversation, or data exchange, involves a non-American located outside the US at the time of collection."[37] A new policy in 2008 detailed in "Defense Supplemental Procedures Governing Communications Metadata Analysis," authorized by Defense Secretary Robert M. Gates and Attorney General Michael B. Mukasey, said that since the Supreme Court had ruled that metadata was not constitutionally protected, N.S.A. analysts could use such information "without regard to the nationality or location of the communicants"[38]

Returning to examples from Europe, under TEMPORA we are presented with the case of an intelligence agency based in the EU (GCHQ of the UK) which is going far beyond mere metadata but which in the first instance for a period of at least three days records contents of e-mail and telephone calls and traces of web searches and on-line activity on a previously unimaginable scale. These activities by SIS may fall outside the scope of EU law on account of Art 4 sect 2 but how do they sit in the context of the Council of Europe's Convention 108?

A few reminders of what Convention 108 actually stipulates would appear to be useful at this stage:

In Article 1 we find that, unlike FISA in the United States, the European Data Protection Convention does not makes any distinction based on nationality or residence but specifies that "The purpose of this convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection")".

After laying out the now "standard" safeguards in Articles 5 – 8, it is in Article 9 of Convention 108 that we find important provisions that apply to both LEAs and SIS. Firstly we find the exception:

> No exception to the provisions of Articles 5, 6 and 8 of this convention shall be allowed except within the limits defined in this article.
>
> Derogation from the provisions of Articles 5, 6 and 8 of this convention shall be allowed when such derogation is provided for by the law of the Party and constitutes a necessary measure in a democratic society in the interests of:
>
> protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences;

36 Ibid.

37 James Ball "NSA stores metadata of millions of web users for up to a year, secret files show" theguardian.com, Monday 30 September 2013 17.35 BST last accessed on 30 September 2013 at http://www.theguardian.com/world/2013/sep/30/nsa-americans-metadata-year-documents

38 JAMES RISEN and LAURA POITRAS, N.S.A. Gathers Data on Social Connections of U.S. Citizens, New York Times 28 September 2013 infra. last accessed on 30 September 2013 The legal underpinning was "a 1979 Supreme Court ruling that Americans could have no expectation of privacy about what numbers they had called. Based on that ruling, the Justice Department and the Pentagon decided that it was permissible to create contact chains using Americans' "metadata," which includes the timing, location and other details of calls and e-mails, but not their content. The agency is not required to seek warrants for the analyses from the Foreign Intelligence Surveillance Court"

protecting the data subject or the rights and freedoms of others.

The key safeguards laid out in Article 9 are that the derogation must a) be provided for by law and b) is proportional. Indeed some would argue that the test set by the Convention is higher than mere proportionality: a measure must be necessary: "Must have" rather than "nice to have".

If one were to use TEMPORA as a case study, does it meet the requirements of "provided for by law" and absolutely "must have"? Findings by the Dutch Intelligence agency[39] suggest that much terrorist activity does not occur at the surface level of internet transactions where most citizens – and search engines – operate but rather in the "Undernet" or "Deep Web". For example the Dutch findings suggest that an Islamist Web underground is centered around "core forums." These websites are part of the Deep Web, or Undernet, which is name given to the multitude of online resources not indexed by commonly used search engines and where communications are often encrypted. The Dutch report published in 2012 and other sources suggest that only 0.2 per cent of the Internet can be searched. [40] If this analysis is correct then not only would PRISM and TEMPORA appear to be disproportionate responses but also that they can in no way be classified as necessary. Indeed it has been suggested that the "infrastructure set up by the National Security Agency, however, may only be good for gathering information on the stupidest, lowest-ranking of terrorists. The Prism surveillance program focuses on access to the servers of America's largest Internet companies, which support such popular services as Skype, Gmail and iCloud. These are not the services that truly dangerous elements typically use."[41] So much so that commentators such as Bershidsky have advocated that "Even complete access to these servers brings U.S. authorities no closer to the core forums. These must be infiltrated by more traditional intelligence means, such as using agents posing as jihadists or by informants within terrorist organizations. Similarly, monitoring phone calls is hardly the way to catch terrorists. They're generally not dumb enough to use Verizon."[42]

Yet, in spite of such considerations on proportionality and necessity, the European-based TEMPORA project may probably be working against the spirit and the letter of European law but not necessarily outside the boundaries of UK law. The most recent debates in the UK media and analysis of English law such as RIPA[43] would suggest that there is some element of wide generic legal provision but the jury is still out on whether this is unreasonably wide[44] and generic, or whether the currently applicable oversight mechanisms in the UK are up to the task of providing adequate measures of protection from unwarranted intrusion into citizen privacy. Even the Chairman of the UK Parliament's Intelligence & Security Committee has most recently gone on record to admit that:

39 General Intelligence and Security Service, Ministry of the Interior and Kingdom relations, "Jihadism on the Web, A breeding ground for Jihad in the modern age".last accessed on 24 September 2013 at https://www.google.com.mt/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&cad=rja&ved=0CD0QFjAC&url=https%3A%2F%2Fwww.aivd.nl%2Fpublish%2Fpages%2F2402%2Fhet_jihadistisch_internet_eng.pdf&ei=rvdLUsesK4-Lswb66oDQCw&usg=AFQjCNFrv3X-s8ufi0wa2NQpraP-gqQqYg

40 He, Bin; Patel, Mitesh; Zhang, Zhen; Chang, Kevin Chen-Chuan (May 2007). "Accessing the Deep Web: A Survey". Communications of the ACM (CACM) 50 (2): 94–101. doi:10.1145/1230819.1241670.

41 Leonid Bershidsky, U.S. Surveillance Is Not Aimed at Terrorists, Bloomberg June 23 2013, last accessed on 24 September 2013 at http://www.bloomberg.com/news/2013-06-23/u-s-surveillance-is-not-aimed-at-terrorists.html

42 Ibid.

43 Regulation of Investigatory Powers Act 2000, UK.

44 An almost incredibly wide power available under UK law is to be found within Section 7 of the Intelligence Services Act whereby the Minister can effectively authorise GCHQ to break UK law in relation to anything appearing to originate from [overseas] apparatus. The precise text is 1") If, apart from this section, a person would be liable in the United Kingdom for any act done outside the British Islands, he shall not be so liable if the act is one which is authorised to be done by virtue of an authorisation given by the Secretary of State under this section" last accessed on 24 September 2013 at http://www.legislation.gov.uk/ukpga/1994/13/section/7

> "There are real issues that do arise out of the Snowden affair, in Britain as elsewhere. Even if the intelligence agencies always act within the law, it must be right for that law to be reviewed from time to time to see whether the safeguards are adequate. Sometimes they are not. The intelligence and security committee criticised the government's original proposals for closed proceedings in civil actions as being wider than was necessary. We have criticised some of the provisions in the proposed Communications Data Bill.
>
> There has also been a crucial need for greater powers for the committee. That has now been conceded by the government. As of this autumn, the intelligence agencies can no longer refuse it any information it seeks. We now have the statutory power to investigate MI6, MI5 and GCHQ operations, which we did not have in the past. Our budget is being almost doubled to £1.3m and our staff are being greatly strengthened."[45]

These comments by Malcolm Rifkind actually go to the heart of the matter: it is not that the law may not exist but rather is it still adequate for the current situation and are the means of oversight and resources allocated for enforcement appropriate? It is clear that what is actually required in Europe, at the level of the Council of Europe and elsewhere, is a healthy open debate about the adequacy of existing safeguards, necessity and proportionality of current practices, best practices, resources, structures and procedures of oversight mechanisms. For the research within the PUPIE project as referred to previously suggests that SIS across Europe are not always dealt with in comparable terms and that their access to and use of personal data would benefit greatly from a significant level of harmonisation. What then would be the legal instrument capable of most rapidly delivering such harmonisation? An EU Directive/Regulation negotiated in Brussels or a binding legal instrument produced in Strasbourg within the wider ambit of the 47-member state Council of Europe?

The fact that member States of the Council of Europe have reported that data collected for state security purposes is subjected to data protection rules in terms of Convention 108 does not mean that the same standards of protection are achieved across all European states or that these standards are high enough. The extent to which oversight mechanisms may lack adequacy and may not be working at comparable levels is also highlighted by the most recent statements of the German Federal Data Protection Commissioner Peter Schaar. On the same day of September 2013 when Malcolm Rifkind was publicly taking critics to task in the UK media as to the level of legal protection actual existing in the UK, one finds the German media reporting that "Since whistleblower Edward Snowden revealed the methods of the US intelligence gathering service, NSA, Schaar says he has felt let down by the German government. He says he cannot assess the role played by the German intelligence services in the scandal because the German interior ministry says it is not his jurisdiction."[46] He went on to say that "a lack of transparency in public authorities' activities could lead to a loss of trust in democracy itself".[47]

This issue of transparency is also clearly not a major source of concern within Europe alone. The US President's reaction to the torrent of public concern unleashed by Snowden's revelations was to announce a number of initiatives aimed at bolstering transparency: "It's not enough for me as president to have confidence in these programs," Obama declared at a White House news conference. "The American people have to have confidence as well."

---

45 Rifkind, Malcolm. 2013. What rubbish, Sir Simon! Our intelligence agencies are not outside the law. The Guardian. Accessed at http://www.thequardian.com/commentisfree/2013/sep/20/rubbish-sir-simon-intelligence-snowden

46 Fürstenau, Marcel. "Transparency lacking, says top data watchdog", Deutsche Welle, 21 Sep 2013 last accessed on 24 Sep 2013 at http://www.dw.de/transparency-lacking-says-top-data-watchdog/a-17104023

47 Ibid.

Among other things, Obama called for the creation of an outside task force to advise his administration on how to balance civil liberties and security issues. He also said he had directed the intelligence community to make public as much information about the spying programs as possible and directed the NSA to create a website that would be a "hub" for that information. "These steps are designed to make sure the American people can trust that our interests are aligned with our values," Obama said."[48]

When striving towards greater transparency and contemplating new mechanisms aimed at advising on how better to achieve a balance between security and civil liberties such as privacy the US administration would appear to be moving in directions which would be very much aligned with the current political mood in much of Europe. Likewise, it would be very surprising if the values of US citizens[49] would not align themselves with those of EU citizens. Reference should here be made to the findings of *inter alia* the CONSENT and SMART Research projects about the perceptions of citizens and their attitudes to privacy and surveillance. In SMART emerging results[50] from research carried out in a number of EU Member States suggest that European citizens are very unhappy about integrated large scale dataveillance and especially being unconsciously "spied upon"[51] by either the state or private companies. Forthcoming research[52] may help establish more precisely as to whether citizens actually care as to whether they are being spied upon by their own state or by a foreign state but one would not be surprised if most citizens would turn out to be upset either way if they feel that their privacy is being infringed upon in a disproportionate and unnecessary manner.

In all of the three examples cited above, the UK, Germany and the USA there is clearly a call for action with varying degrees of dissatisfaction with the current national levels of adequacy of safeguards, oversight and resources available for enforcement. If gauged by reactions in the media or public statements from data protection authorities and some politicians it would be fair to say that the situation and mood across most European states in September 2013 is not dissimilar to that in these three prominent members of the G20. So, the question naturally arises, would it be helpful and possible for joint action at the international level to develop a satisfactory way forward? Within a European context, to continue reflecting on the opportunity afforded to us by the UK case study in TEMPORA, there may be areas where the other 46 member States of the Council of Europe may stand to learn quite a few things from the UK's experience and vice-versa. It would not be unreasonable to assume that the development of a set of legally-enforceable – and enforced – safeguards, oversight mechanisms and resourcing levels common to all European states would also improve the international collaboration to fight crime and terrorism which is increasingly required in the Internet era. This goal remains difficult to achieve but is not beyond the realms of the imagination. Long years of mutual mistrust will need to be overcome but the alternatives - technical counter-measures at national and regional levels, parallel internets, refusal to collaborate or exchange information, boycott of whole swathes of existing fibre-optic cables and cloud service providers – could prove to be a far more damaging prospect than a common

48 Bailey, Holly. 2013. Obama speaks out on Snowden, calls for greater transparency on surveillance. Yahoo News. Accessed at http://news.yahoo.com/obama-to-hold-white-house-news-conference-164610288.html

49 See for example the findings about how US citizens feel about the balance between surveillance, terrorism and privacy as reported in JENNIFER AGIESTA, DIGITS: Torn between civil liberties, terrorism, Associated Press, 17 September 2013 last accessed on 24 September 2013 at http://bigstory.ap.org/article/digits-ambivalence-civil-liberties-terrorism

50 Brockdorff, Noellie, Sandra Appleby Arnold, Christine Garzia et al. European citizens' perspective of smart dataveillance: preliminary results from Work Package 10 of the SMART project. Presented at Intelligent Investigation Policy Workshop conference http://www.iri.uni-hannover.de/programme.html on 19 September, 2013, Brussels. Final report to be put into the public domain in 2014.

51 See Deliverable D10. in the SMART project. In these findings citizens are actually more upset if the "surveillance" is carried out by private companies than by the state. To be made available on-line at www.smartsurveillance.eu by May 2014.

52 E.g. in WP12 of the RESPECT project http://respectproject.eu/

European or indeed international approach to data protection in the case of security and intelligence services. Of course the debate will continue to be muddled further by the complications induced by espionage for economic reasons or cyber-warfare but this is no reason to avoid having a calm, well-reasoned Europe-wide discussion on improving the currently available set of safeguards. The European discussion would only be a start for many other states outside Europe, not least long-standing allies like the United States, Canada, Australia and New Zealand, not to mention a whole host of emerging and established economies would doubtless be keener to adopt comparable and compatible measures rather than go for alternatives which might involve the "balkanisation" of the internet, perennial economic espionage and cyber-warfare.

If one were to reflect even further on TEMPORA as a case study it is clear that part of the surveillance programme could be a matter of either lawful or unlawful interception of data with the lawfulness or otherwise depending very much on the existing state of legislation in a given European state. This would not necessarily constitute public/private data sharing as most probably originally intended by the brief though it could give rise to intelligence data that might possibly be shared across borders. It has been alleged[53] that a number of private sector firms have been complicit with the SIS in enabling them to obtain data. In June 2013 it was alleged that the NSA was collecting "directly from the servers of these U.S. Service Providers: Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, Apple."[54] These claims have been denied with varying degrees of strength but "Each of the statements issued by Google, Facebook and other companies linked to the program has been carefully worded in ways that doesn't rule out the possibility that the NSA has been gathering online communications as part of its efforts to uncover terrorist plots and other threats to U.S. national security." [55] The wording of the statements by the largest firms in the private sector is such as to give credence to the assessment "I think a lot of people are spending a lot of time right now trying to parse those denials…The top level point is simply: it's pretty hard to know what those denials mean."[56]

One of the earlier interviews with Snowden contained explicit questions about various forms of co-operation between the public and private sectors:

> Interviewer: Do private companies help the NSA?
> Snowden: Yes. Definitive proof of this is the hard part because the NSA considers the identities of telecom collaborators to be the jewels in their crown of omniscience. As a general rule, US-based multinationals should not be trusted until they prove otherwise.[57]

Why this situation has come about in a country like the United States about has probably been captured most succinctly in the following analysis by Bruce Schneier:

> "The result is a corporate-government surveillance partnership, one that allows both the government and corporations to get away with things they couldn't otherwise. There are two types of laws in the U.S., each designed to constrain a different type of power: constitutional

53Glenn Greenwald and Ewen MacAskill "NSA Prism program taps in to user data of Apple, Google and others" The Guardian, Friday 7 June 2013 last accessed on 24 September 2013 at http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

54 Barton Gellman and Laura Poitras, U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program" The Washington Post Published: June 6 | Updated: Friday, June 7 last accessed on 24 September 2013 at http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html

55 DigTriad, Fighting Terrorism Using Metadata from Web Users last accessed on 24 September 2013 at http://www.digtriad.com/news/local/article/287663/57/Government-Collecting-Metadata-on-Web-Users

56Ibid. citing Lee Tien, a senior staff attorney at the Electronic Frontier Foundation, a digital rights group

57 The NSA and Its Willing Helpers Der Spiegel On-line 07/08/2013 03:34 PM last accessed on 24 September at http://www.spiegel.de/international/world/interview-with-whistleblower-edward-snowden-on-global-spying-a-910006.html

law, which places limitations on government, and regulatory law, which constrains corporations. Historically, these two areas have largely remained separate, but today each group has learned how to use the other's laws to bypass their own restrictions. The government uses corporations to get around its limits, and corporations use the government to get around their limits.

This partnership manifests itself in various ways. The government uses corporations to circumvent its prohibi1ons against eavesdropping domestically on its citizens. Corporations rely on the government to ensure that they have unfettered use of the data they collect.

Here's an example: It would be reasonable for our government to debate the circumstances under which corporations can collect and use our data, and to provide for protections against misuse. But if the government is using that very data for its own surveillance purposes, it has an incentive to oppose any laws to limit data collection. And because corporations see no need to give consumers any choice in this matter -- because it would only reduce their profits -- the market isn't going to protect consumers, either.

Our elected officials are often supported, endorsed and funded by these corporations as well, setting up an incestuous relationship between corporations, lawmakers and the intelligence community."[58]

The importance of such public-private surveillance partnerships was highlighted in some of the latest revelations from Snowden which suggest that the NSA "was using its metadata troves to build profiles of US citizens' social connections, associations and in some cases location, augmenting the material the agency collects with additional information bought in from the commercial sector, which is not subject to the same legal restrictions as other data."[59] Here it should be noted that a "top-secret document titled "Better Person Centric Analysis" describes how the agency looks for 94 "entity types," including phone numbers, e-mail addresses and IP addresses. In addition, the N.S.A. correlates 164 "relationship types" to build social networks and what the agency calls "community of interest" profiles, using queries like "travelsWith, hasFather, sentForumMessage, employs…. A 2009 PowerPoint presentation provided more examples of data sources available in the "enrichment" process, including location-based services like GPS and TomTom, online social networks, billing records and bank codes for transactions in the United States and overseas"[60]

Like its counterpart GCHQ in the UK, the "NSA also collects enormous quantities of metadata from the fibre-optic cables that make up the backbone of the internet. The agency has placed taps on undersea cables, and is given access to internet data through partnerships with American telecoms companies. About 90% of the world's online communications cross the US, giving the NSA what it calls in classified documents a "home-field advantage" when it comes to intercepting information."[61]

Against this background, it is not difficult to understand how permeable the "wall" may be between SIS and LEA activities and how the purpose of collection whether serious crime or

58 Bruce Schneier "The Public/Private Surveillance Partnership" August 5 2013, last accessed on 24 September 2013 at https://www.schneier.com/blog/archives/2013/08/the_publicpriva_1.html

59 JAMES RISEN and LAURA POITRAS, N.S.A. Gathers Data on Social Connections of U.S. Citizens, New York Times 28 September 2013 last accessed on 30 September 2013

60 Ibid.

61 James Ball "NSA stores metadata of millions of web users for up to a year, secret files show" theguardian.com, Monday 30 September 2013 17.35 BST last accessed on 30 September 2013 at http://www.theguardian.com/world/2013/sep/30/nsa-americans-metadata-year-documents

national security may be resident in one and the same process. The following extract from another part of the Snowden interview cited earlier offers an insight into the real world of how intelligence is used:

> Interviewer: Are German authorities or German politicians involved in the NSA surveillance system?
>
> Snowden: Yes, of course. We're in bed together with the Germans the same as with most other Western countries. For example, we tip them off when someone we want is flying through their airports (that we for example, have learned from the cell phone of a suspected hacker's girlfriend in a totally unrelated third country -- and they hand them over to us. They don't ask to justify how we know something, and vice versa, to insulate their political leaders from the backlash of knowing how grievously they're violating global privacy.

Is this also a type of transfer of data generated primarily in the private sector outside Europe that we should be thinking of in terms of the brief? If so we are clearly in something of a pickle: Both non-European and European SIS are gathering several thousand petabytes of metadata and content every day. Whatever the claims for sifting out data, they sometimes share this data with LEAs "The ability to look back on a full year's history for any individual whose data was collected – either deliberately or incidentally – offers the NSA the potential to find information on people who have later become targets. But it relies on storing the personal data of large numbers of internet users who are not, and never will be, of interest to the US intelligence community."[62]

Once again this brings us back to the key questions: Is storing the personal data of large numbers of internet users who are not, and never will be, of interest to the US intelligence community or indeed any European intelligence community

i. a manageable risk to privacy?
ii. a proportionate measure in a democratic society?
iii. a necessary measure in a democratic society?

11 Conclusions

Basically, the picture which has emerged by end September 2013 is of a world where the lines between gathering of personal data for criminal justice purposes and intelligence or national security purposes are increasingly blurred. A number of fresh realities have to be dealt with by the policy-maker:

1. Private citizens across and outside Europe carry out billions, possibly trillions of on-line transactions with each other and commercial corporations every day using value-added services and communication routes provided almost exclusively by the private sector

2. The legitimate on-line transactions of private citizens are carried out within the same on-line environment where various forms of cybercrime are carried out, where serious organised crime may be using or "hiring out" sophisticated forms of cyber-attacks (including botnets) and where intelligence services may be carrying our cyber-espionage, counter-espionage and where nation states may also be contemplating or carrying out cyberwarfare. In this respect, the cyber eco-system may be compared to a "digital soup", not a "digital minestrone" where different individual components may be more easily recognised and identified, but a finely blended digital puree consisting of bits

62 Ibid.

and bytes by the petabyte which could variously be part of e-commerce, social networking, cybercrime, cyber-espionage or cyberwarfare. Threat intelligence may be obtained and shared across borders after a careful microscopic forensic analysis of this "digital soup". Given that the commercial size, financial muscle and data processing capabilities of a small number of multinational corporations matches or exceeds that of the SIS of most nations, this threat intelligence may often also be generated by the private sector or by SIS with access to data held by the private sector.

3. Whatever transactions being carried out by private citizens on-line are, in practice, considered to be "fair game" by the SIS of some of the most highly industrialised countries, many of them members of both the Council of Europe and the European Union. Fingers have been pointed at the SIS of the UK, Germany, France and the Netherlands in addition to the NSA in the United States where evidence suggests that increasingly sophisticated technological means are being developed and deployed to maintain constant analysis of the "digital soup" that is the Internet.

4. While in the EU traffic data is retained for 6-24 months in terms of the Data Retention Directive, in the USA this time-period for records which could possibly be even more content-rich than its European counterpart could be up to ten years;

5. Available evidence suggests that there is an increasing trend for all data going through fiber-optic cables in both the UK and the USA to be possibly subjected to the equivalent of "indiscriminate vacuuming" and retained for a period of at least three days before being filtered down into more manageable and digestible portions with the metadata then being tucked away for anything between at least two months and a year.

6. The transactions of citizens everywhere and anywhere which are somehow tapped into indiscriminately by the SIS of technically advanced and geographically strategically well-positioned[63] nations are not only stored in various forms but are subjected to an ever-increasing number of types of automated and manual analysis which includes the creation of various ways of profiling of citizens and attempts to draw out their social networks from a very detailed set of over 94, sometimes over 150 indicators or data types

7. Whereas police forces and other forms of LEAs may most often be constrained by diminishing financial resources and data protection law safeguards, such constraints do not appear to exist for the increasingly well-funded and relatively "soft-touch regulated" SIS who then however very regularly feed the LEAs with various actionable personal data. Likewise, personal data processed by corporations located in countries with less stringent data protection laws may help circumvention of such laws by both LEAs and SIS by carrying out the processing out of reach of European-standard data protection laws and then communicating threat-intelligence at will to chosen partners internationally irrespective of whether these partners are also in the private sector or belong to LEAs or SIS.

8. More and more data being fed to the criminal justice sector is coming from the security and intelligence sector (SIS) and directly or indirectly from the private sector. This is being done internationally on a scale previously unimaginable and there exist serious concerns that not only is the intrusion into the lives of citizens disproportionate and unnecessary but also that unless an adequate legal framework is in place then some or

63 i.e. where the fiber optic cables or the data traffic happen to be passing

much of the intelligence gathered from on-line personal data would not be admissible in a court of law and the number of successful prosecutions would be minimal.

9. Any concerns over data protection regulations in relation to transborder private/public information sharing for (a) network security purposes and (b) criminal justice purposes must be considered in the wider context of the realities of the collection of personal data and its use by BOTH LEAs and SIS. In the end it is the same personal data generated by the same private citizens through the same transactions using the same browsers and search engines over the same ISPS and other service providers. Available evidence suggests that citizens do care about being watched and are increasingly aware that the watchers are a mix of for-profit corporations, organised crime, LEAs and SIS. They are also aware that in many situations in many countries LEAs and SIS work closely together and their acceptance of the use of such data or other current practices should not be taken for granted. There is growing evidence[64] which suggests that there is an acute difference between public awareness of personal data processing practices by LEAs ad SIS and the citizens' acceptance of such practices. The debate may be just starting and if public mobilisation in the case of ACTA is anything to go by the possible effect of this incipient public debate should not be under-estimated.

10. There is also a growing shift by legislators and other policy makers in both North America [65]and Europe[66] to reconsider the legal empowerment and financial resourcing to LEAs and SIS in regard to their legal and technical capability to process huge amounts of personal data.

The above considerations should be made against some stark legal realities. The Council of Europe, within its Data Protection Convention and/or within the Cybercrime Convention has both the legal framework and the credibility to explore the development of a tripod of measures aimed at achieving the balance between privacy and security or crime detection and prevention:

---

64 See much of the quantitative and qualitative research gradually being released into the public domain by EU FP7-supported research projects such as CONSENT, SMART and RESPECT.

65 The author of the PATRIOT Act in the USA, Rep. Jim Sensenbrenner displayed grave concern over the use of Section 215 of that law to justify the collection of personal data and at a July 2013 hearing of the House Judiciary Committee, berated Deputy Attorney General James Cole on the US government's interpretation of Section 215: Section 215 requires the government to certify that its information requests are relevant to an ongoing terrorist investigation. But Sensenbrenner notes that the government claims that records of every phone call in America is relevant to a terrorism investigation. He asked: "Doesn't that make a mockery of the legal standard, because you're trying to have it both ways?"

Cole insisted the government wasn't trying to have it both ways. But Sensenbrenner wasn't satisfied.

"You sure are because you're saying have the court authorized to get the records of all the phone calls that are made to and from phones in the United States including people who have nothing to do with any kind of terrorist investigation.

"You gobble up all of those records and then you turn around and say well we'll pick out maybe 300 phone numbers out of the billions of records that you have every day and you store for five years there," he said. "All the rest of this stuff is sitting in a warehouse and we found out from the IRS who knows who wants to have any kind of legal or illegal access to it. You are having it both ways."

"Section 215 expires at the end of 2015," Sensenbrenner warned Cole. "Unless you realize you've got a problem, that is not going to be renewed. There are not the votes in the House of Representatives to renew Section 215. You have to change how you operate Section 215, otherwise in two and a half years you're not going to have it any more." Abstracted from Timothy B. Lee "Whoa: Watch the PATRIOT Act's

author warn Congress might cancel the spying program" in the Washington Post 17 July 2013 last accessed on 24 September 2013 at http://www.washingtonpost.com/blogs/wonkblog/wp/2013/07/17/whoa-watch-the-patriot-acts-author-warn-congress-might-cancel-the-spying-program/

66 Jan Philipp Albrecht, Green MEP and Rapporteur on the Data Protection Regulation in the European Parliament's LIBE Committee has commented to this effect in many instances including http://www.theparliament.com/latest-news/article/newsarticle/prism-jan-philipp-albrecht/#.Uku9kBDl5To

1 Adequate legal safeguards;
2 Meaningful Oversight Mechanisms;
3 Sufficient resources for effective enforcement.

An additional protocol to either Convention or possibly an entirely new Convention – i.e. one or more of the three options outlined in greater detail in the Recommendations made in the separate study[67] – may be a viable way forward in the current political climate.

Such a way forward for the 47 member States of the Council of Europe would meet the triple imperatives of a) the modernisation of R(87)15, b) the modernisation of Convention 108 and c) a proportionate reaction to the public outcry following the Snowden revelations. It would not be incompatible with the options open to the member States of the Council of Europe who also happen to be EU Member States. The result would contain detailed rules about public-private data sharing including the scenarios and realities examined above. These would conceivably be brought together in a binding legal instrument – or indeed possibly a family of legal instruments - capable of being deployed both inside and outside Europe.

67 Report Recommendation R (87) 15 – Twenty–five years down the line by Professor Joseph A. Cannataci and Dr. Mireille M. Caruana submitted for consideration by the Council of Europe's Consultative Committee on Data Protection T-PD, cited supra.