DP(2014)01

Strasbourg, 8 September 2014

Key points regarding access to personal data by law enforcement and by national security agencies

Report

By Joseph A. CANNATACI (Malta)

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

andGraham SUTTON (United Kingdom)

Independent Data Protection Expert, Former Policy Adviser, Department of Constitutional Affairs, Ministry of Justice

Directorate General of Human Rights and Rule of Law

Executive summary

- Article 8 of the European Convention on Human Rights (ECHR) provides for the right to private life. Interception of communications is not necessarily incompatible with that right, but it must be carried out consistently with the requirements both of the ECHR and the Council of Europe Data Protection Convention.
- In the UK, interception of communications by the law enforcement or intelligence agencies is carried out under the Regulation of Investigatory Powers Act 2000 (RIPA). Authorisation for interception can be given by a Cabinet Minister in limited circumstances. RIPA also regulates access to communications data that have already been stored.
- The European Court of Justice (ECJ) has declared invalid the EU Data Retention Directive which required EU Member States to retain communications data for a specified period for the purpose of combating serious crime. The ECJ was not opposed to the principle of data retention but was concerned about certain of the specific arrangements.
- A recent Vodaphone report has highlighted the undesirable practice of law enforcement and intelligence agencies being enabled to carry out interception activities without the agreement or knowledge of the service operator.
- Making publicly available statistical information about interception is important to securing public confidence in the arrangements.
- Independent, preferably judicial, oversight mechanisms are necessary,
- Law enforcement agencies and security agencies should generally be subject to the same arrangements.

Introduction

This report responds to a request from the Parliament of Georgia for information about the circumstances in which it may be legitimate for law enforcement or intelligence agencies to gain access to communications transmitted electronically. Part I of the paper sets out the effect of Article 8 of the European Convention on Human Rights and data protection rules. It goes on to describe the statutory arrangements in the United Kingdom. Finally, it refers to the recent judgement of the European Court of Justice on the EU Data Retention Directive. Part II of the report looks more closely at the practical arrangements and safeguards for interception, referring in particular to a recent report by Vodaphone. It concludes with a number of recommendations.

The report is prepared by the following scientific experts:

- Joseph A. Cannataci, who is a European information policy and technology law expert working closely on these issues with the Council of Europe and the European Union. As a Council of Europe expert, he has carried out expert missions in a number of countries including Bulgaria, Czech Republic and Ukraine. Over the past quarter of a century he has served as Chairman of several Committees of Experts of the Council of Europe: MedialLex (1994), Working Party on Data Protection in Insurance (1994-1997), Working Party on Data Protection in New technologies (1995-2000), the Committee of Experts on Data Protection (1996-98) and Vice-Chairman of the Group of Specialists on the impact of New Communications

Technologies on Fundamental Rights & Democratic Values (1999-2001). Most recently he has been Expert Consultant to the Council of Europe's Consultative Committee on Data Protection responsible for drawing up the report (2011-2013) on data protection in the police sector and to the Council of Europe's Cybercrime division preparing an analysis on data protection and network security (2012-2013). He is the chief architect and overall scientific coordinator of several recent or current major EU-funded research projects dealing with privacy and surveillance, including CONSENT, SMART and RESPECT. For the purposes of this analysis, Professor Cannataci also enjoyed the close collaboration of a team member and colleague, Dr OleksandrPastukhov, with close knowledge of data protection in the emerging democracies of Central and Eastern Europe.

- Graham Sutton, who formerly worked for the UK civil service where he spent twelve years in charge of data protection policy. Since taking early retirement in 2004, he has continued to work on data protection as a free-lance consultant. Among other things, he has advised on the development of data protection policy in China as well as a number of the new democracies in central and eastern Europe.

Part I

Article 8 of the European Convention on Human Rights and data protection

Article 8.1 of the European Convention on Human Rights (ECHR) provides that: "Everyone has the right to respect for his private and family life, his home and his correspondence." Article 8.2 provides some closely focused derogations from that right. It says: "There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

In considering whether an activity is in breach of Article 8, it is necessary first to establish whether there has been an interference with the rights established by that article. Case law of the European Court of Human Rights establishes that covert interception of electronic communications does represent an interference with the right to private life (see, for example, the judgments in *A v France* of 23 November 1993, or *Halford v United Kingdom* of 25 June 1997). For the interference to be legitimate, it needs to be shown that it comes within the scope of the exemptions in Article 8.2.

- The interference must be in accordance with the law. It must have a valid basis in domestic law; the law in question must be accessible to the individual; and the consequences of the law must be foreseeable for the individual. "Foreseeable" means that the law must be precise enough for the individual to regulate his/her conduct.
- The interference must have a legitimate aim. It must come within one of the aims set out in Article 8.2.

- The interference must be necessary in a democratic society. It must correspond to a pressing social need; and be proportionate to the legitimate aim pursued.

The interception of communications for law enforcement or intelligence purposes is not necessarily inconsistent with the ECHR. Indeed, some international legal instruments impose a duty on contracting states to employ special investigative measures such as the interception of communications to combat certain forms of crime.[1]Nonetheless, that duty has to be balanced against the need to respect for individuals' rights under Article 8. In its preamble, Council of Europe Recommendation R(87)15 on the use of personal data in the police sector stresses the need to strike a balance between law enforcement objectives and individuals' rights, in particular their right to private life: "Recognising the need to balance the interests of society in the prevention and suppression of criminal offences and the maintenance of public order on the one hand and the interests of the individual and his right to privacy on the other."

The rules on data protection, set out in the 1981 Council of Europe Data Protection Convention and the additional Protocol to that Convention (and currently under review), derive from the right to private life established by Article 8 of the ECHR. Information about or obtained from electronic communications by law enforcement or intelligence agencies will almost certainly include, indeed is likely largely to comprise, personal data. The rules on data protection should, therefore, be applied to the collection and further processing of such data, subject only to the need to provide derogations to safeguard legitimate interests. Article 9 of the Data Protection Convention permits derogations where they constitute: "...a necessary measure in a democratic society in the interests of:

a. protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences;
b. protecting the data subject or the rights and freedoms of others."

The position in the United Kingdom

In the United Kingdom the principal legislation governing surveillance is the Regulation of Investigatory Powers Act 2000 (RIPA). RIPA covers a range of activities by a variety of agencies. This report deals only with its impact upon the law enforcement and intelligence agencies as regards the interception of electronic communications, and access to communications data. The description that follows does not give a complete picture of RIPA's scope. Moreover, the description is in general terms, and should not be taken as a precise statement of the law. It is offered to provide a broad picture of the position in the UK. In considering the description that follows, it should be borne in mind that in carrying out their functions the law enforcement and intelligence agencies, like all other private and public sector bodies, are bound by the provisions of the United Kingdom's data protection legislation, the Data Protection Act 1998.

[1] See, for example, the Council of Europe Criminal Law Convention on Corruption

Interception of electronic communications

RIPA makes it a criminal offence, intentionally and without lawful authority, to intercept any communication in the course of its transmission by a public or private telecommunications service.The maximum penalty for the offence is two years' imprisonment or an unlimited fine. Prosecution may take place only with the consent of the Director of Public Prosecutions.

One of the ways in which interception has lawful authority is when it is carried out in accordance with a warrant issued by the Secretary of State (that is to say a Cabinet Minister and the political head of a Government Department). A warrant must not be issued unless the Secretary of State believes it to be necessary on one of the following grounds:

- In the interests of national security
- For the purpose of preventing or detecting serious crime (including giving effect to international mutual assistance agreements)
- For the purpose of safeguarding the economic well-being of the United Kingdom

The conduct authorised by the warrant must be proportionate to the objective of issuing the warrant.There is a duty on the Secretary of State to consider whether the information sought could be obtained by other means.RIPA specifies a relatively short list of persons who may apply for warrants. These include the heads of the intelligence services and the heads of certain police agencies. Warrants must be signed by the Secretary of State in person, or in urgent cases by a senior official but only with the Secretary of State's authorisation.

RIPA sets out detailed provision relating to the content of warrants, their duration, renewal, modification etc. Specifically, a warrant must be closely focused, naming only one person or one set of premises as the target of interception.

There is a power for the Secretary of State to require service operators to provide assistance in the implementation of warrants; and the Secretary of State is under a duty to pay a fair contribution towards the costs incurred by service operators.

RIPA sets out safeguards in relation to the product of interception. These require that the extent to which the product is disclosed and copies made is kept to the minimum; that the product must be kept secure; and that the product is destroyed as soon as it is no longer necessary to retain it for the purpose for which the warrant was issued.

The product of interception is not admissible as evidence in court. There is a duty on all involved to keep all information about warrants (including their existence) secret. Not to do so is an offence.

Obtaining and disclosing communications data

In addition to dealing with interception, RIPA also deals with access to communications data (that is data relating to a telephone call, an e-mail or a visit to a website) that have already been collected and stored. "Communications data" covers traffic data as well as information about the service used and the subscriber, but does not include the content of communications.

RIPA allows the obtaining and disclosure of communications where authorisation has been given. Authorisation may be given by people holding a rank designated by the Secretary of State, within specified public authorities. The public authorities include the intelligence services and police forces as well as other entities. The Secretary of State has the power to specify public authorities for this purpose.

Authorisation may be given where a designated person believes it is necessary forone of a number of purposes. These include, among others, the interests of national security and the prevention or detection of crime, or the prevention of disorder. There is power for the Secretary of State to specify additional purposes. Obtaining the data must be proportionate to the objective in view.

A designated person who believes that a service operator is capable of obtaining communications data, has the power to issue a notice requiring the service operator to do so and to disclose the data to a person specified in the notice.

There is a time limit of one month on authorisations and notices, but they may be renewed.

The Secretary of State is under a duty tomake arrangements for financial contributions towards operators' costs.

Commissioner, Tribunal and Codes of Practice

The Interception of Communications Commissioner, established under RIPA, keeps under review both the way in which the Secretary of State carries out his/her functions in relation to the issue of warrants for interception, and the way in which the functions relating to the obtaining and disclosure of communications data are carried out. The Commissioner has the power to make a report to the Prime Minister when there has been a contravention. The Commissioner must be a judge. (Other Commissioners with different functions in relation to other provisions of RIPA were also established under that legislation.)

RIPA also established the Investigatory Powers Tribunal. In relation to the interception of communications, the Tribunal has the power consider complaints and to investigate whether the procedural requirements for interception under warrant were complied with. It has similar powers in relation to the obtaining and disclosure of communications data. If the Tribunal finds that there has been a contravention, it may impose remedial measures such as the quashing of warrants, the destruction of records, or financial compensation. There is no right of appeal from the Tribunal.

There is a duty on the Secretary of State to produce codes of practice relating to the exercise of the powers and duties in connection with the interception of communications, and the obtaining and disclosure of communications data. Those acting under RIPA have a duty to comply with such codes.

EU Data Retention Directive

The purpose of the EU Data Retention Directive, which was adopted in 2006, was to harmonise the arrangements in the EU Member States for the retention for law enforcement purposes of certain data generated by electronic communications services. The Directive required Member States to provide that such services must retain for periods between 6 months and two years (the exact period to be determined in national legislation) traffic and

location data, and data necessary to identify the subscriber, but not content data. The data were to be made available to the competent national authorities for the purpose of the prevention, investigation, detection and prosecution of serious crime, such as organised crime and terrorism.

In a judgement given in April 2014[2], the European Court of Justice held that the Directive was invalid. It did not condemn the principle of requiring the retention of electronic communications data per se. Indeed, it said that "The retention of data ... is not such as to adversely affect the essence of the fundamental rights to respect for private life and to the protection of personal data". It went on to say that "The retention of data... genuinely satisfies an objective of general interest, namely the fight against serious crime and, ultimately, public security". However, the Court found that the arrangements set out in the Directive "exceeded the limits imposed by compliance with the principle of proportionality". In support of this view the Court said that:

- The Directive was too general in its scope. It failed to provide for any differentiation, limitation or exception as regards the individuals, the means of communication or the traffic data involved, in the light of the objective of fighting against serious crime.
- The Directive failed to set any objective criteria to ensure that national competent authorities could have access to the data only for the purpose of dealing with offences that were sufficiently serious to justify the extent and seriousness of the interference withthe fundamental rights that was involved.
- The retention period was insufficiently precise and lacked objective criteria for limiting it to what was strictly necessary.
- There were insufficient safeguards against the risk of abuse.
- The Directive did not require the data to be retained within the EU and thus within the powers of an independent supervisory authority.

The UK had passed Regulations to give effect to the Directive. In the light of the judgment of the European Court of Justice, the Government has brought forward emergency legislation (the Data Retention and Investigatory Powers Act 2014) to replace the Regulations and bring the arrangements for the retention of communications data in the United Kingdom more into line with the judgment of the Court.

Part II

Further background and intervening circumstances

During the intervening period from the report about the Georgian proposals to up-date the Georgian law on surveillance and interception which was presented by one of the experts of the current report [3], a landmark report [4] was published by a major international communications service provider, Vodafone, which in many ways was the first of its kind by

[2] http://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang=EN

[3] Council of Europe expert's *Opinionon Draft laws of Georgia relating to Surveillance Activities of Law Enforcement Authorities and National Security Agencies*, 14 February 2014

[4] Law Enforcement Disclosure Report 2013-2014, published as part of the Vodafone Group plc Sustainability Report, Page accessed on 02 September at http://www.vodafone.com/content/dam/sustainability/2014/pdf/vodafone_full_report_2014.pdf

such a global operator which provides services in 29 countries. It offers an extremely useful compendium of issues and bad practices to be avoided by any country seeking to up-grade its legislation in this sector. A number of these resonate with any security and technology law expert examining the current situation in Georgia where recent events in May 2014 suggest that telephone snooping especially for political purposes has not been eliminated as a practice.[5]

Key issue 1 – Direct and unfettered technical access

One of the key issues highlighted in the Vodafone report indeed echoed a major problem which had been discussed by the said expert during meetings in Georgia held in March 2014: the direct access to telecom services by a Law Enforcement Agency (LEA) or a Security & Intelligence Service (SIS). To be precise, one is here referring to the ability of the LEA and/or the SIS to use pre-determined technical means to access directly and intercept or otherwise monitor communications without the explicit permission or indeed knowledge of the service operator. In other words the LEA and/or the SIS does not need to go and ask the service operator for a key to "get in" but they would have arranged to have been given the keys in such a way so as to be able to access the technical systems at will. This technical ability should be carefully distinguished from the legality of the access by the LEA or the SIS. It is possible that in some countries, as in the UK, the law may impose an obligation on the LEA and/or the SIS to obtain judicial or administrative permission before being able to use its technical ability to intercept or otherwise monitor communications. Yet, in those countries where the law obliges or practice has evolved that the LEAs and or the SIS are given direct unfettered technical access to the communications, the additional safeguard afforded by a requirement for the service operator to "open the door" does not exist. Put differently, in some European states the LEA and/or the SIS has its own back-door to which it has a key and can go in and out as it pleases, constrained only by the strength or otherwise of the non-technical oversight mechanisms which may exist ina given country. Although this has not been formally independently confirmed by Vodafone, it is understood that Georgia is one of "a small number of countries" where "agencies and authorities have direct access to communications data stored within an operator's network. In those countries Vodafone will not receive any form of demand for communications data access as the relevant agencies and authorities already have permanent access to customer communications via their own direct link"[6]

The fact that this situation is exacerbated by law rather than mitigated may be seen in this explicit reference to legal impositions "in a small number of countries the law dictates that specific agencies and authorities must have direct access to an operator's network, bypassing any form of operational control over lawful interception on the part of the operator".[7] This situation was highlighted by Vodafone's Law Enforcement Disclosure Report published in June 2014 and if Georgia is looking to follow best practice the Vodafone Report has a number of cases which implicitly or explicitly are perfect examples of "what not to do"

[5]Lomsadze G*, Another Phone-Snooping Scandal Smacks Georgia"* in Eurasia news, 13 May 2014, Last accessed on 02 September 2014 at http://www.eurasianet.org/node/68366

[6] Law Enforcement Disclosure Report 2013-2014, published as part of the Vodafone Group plc Sustainability Report, Page 70

[7] Law Enforcement Disclosure Report 2013-2014, published as part of the Vodafone Group plc Sustainability Report, Page 69

as well as very valid recommendations on what to do. The most glaring and relevant is perhaps crystallised in the following recommendation:

> "Amend legislation which enables agencies and authorities to access an operator's communications infrastructure without the knowledge and direct control of the operator, and take steps to discourage agencies and authorities from seeking direct access to an operator's communications infrastructure without a lawful mandate"[8].

Key Issue No 2- transparency

The second important issue is that of transparency. Trust between the citizen, the state and its agencies largely resides on the transparency that exists in a state. An examination of the culture of transparency in Scandinavia and especially in Sweden will probably explain why citizens in those northern States would appear to have more trust in their governments and police forces than in other countries. Yet, one reads that "Law enforcement and national security legislation often includes stringent restrictions preventing operators from disclosing any information relating to agency and authority demands received, including disclosure of aggregate statistics. In many countries, operators are also prohibited from providing the public with any insight into the means by which those demands are implemented"[9]

This is not an approach conducive to confidence in the government, police or security forces in any country and presumably even less so in Georgia where it is clear that public confidence was shaken[10] more than once as a result of the telephone-snooping that appears to have continued to take place.

Would a law explicitly authorising service providers to publish aggregate statistics on the number of requests received resolve the problem? Clearly not since the market is made up of several service providers, none of whom would have the total picture and if left to their own devices would not necessarily compile reports or data with the same rigour or consistency than had a governmental central agency compiled and published the data. Thus, one can support service providers such as Vodafone who argue that for publication of such statistical data to be meaningful it needs to:

- Be independently scrutinised, challenged and verified prior to publication
- Clearly explain the methodology used in recording and auditing the aggregate demand volumes disclosed
- Encompass all categories of demand, or, where this is not the case, clearly explain those categories which are excluded together with an explanation of the rationale supporting their exclusion; and
- Encompass demands issued to all operators within the jurisdiction in question; [11]

The transparency motivator would lend itself to the argument that "disclosure of the number of individual warrants served in a year is currently the least ambiguous and most meaningful statistic when seeking to ensure public transparency"[12]

[8] Law Enforcement Disclosure Report 2013-2014, published as part of the Vodafone Group plc Sustainability Report, Page 70
[9] Law Enforcement Disclosure Report 2013-2014, published as part of the Vodafone Group plc Sustainability Report, Page 62
[10] Tbilisi totally tapped? RT, 21 December 2009, http://rt.com/politics/georgia-wire-tapping-opposition/ on 02 September 2014
[11] Law Enforcement Disclosure Report 2013-2014, published as part of the Vodafone Group plc Sustainability Report, Page 63

This would in turn lend itself to a legislative solution which would make publication of such data mandatory on the Government. Such a task could be actually delegated to or at least independently verified by the national Data Protection Authority which could also be legislatively empowered to request each of the service providers to supply it with their own statistics on an annual basis and then reconcile these reports with the figures reported by the SIS and LEAs. It is important that each judicial warrant be linked to a specific target citizen anonymised through a unique surveillance code in order that no double counting occurs and that one interception or monitoring order on one citizen delivered to, say ten different service providers, would qualify as one warrant for one investigation on one citizen and not ten, thus unnecessarily alarming the public as to the high number of warrants being issued.

Key Issue No 3 – independent oversight mechanisms

The third key issue which would appear to be highly relevant to Georgia is not one that would be given prominence in a service provider's analysis but follows on from the first part of this report which refers to the general situation in the United Kingdom. The position in the UK is described as an example of the arrangements in one Council of Europe member state which is well known to the authors of this paper, and not necessarily as a model to be followed. The oversight mechanism has been very heavily criticised in a number of ways and now for a considerable length of time. The most recent debates in the UK media and Parliament and analysis of English law such as RIPA[13] and oversight mechanisms for its intelligence agencies would suggest that there is some element of wide generic legal provision but the jury is still out on whether this is unreasonably wide[14] 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:

- 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

[12] Law Enforcement Disclosure Report 2013-2014, published as part of the Vodafone Group plc Sustainability Report, Page 64

[13] Regulation of Investigatory Powers Act 2000, UK.

[14] 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

> not have in the past. Our budget is being almost doubled to £1.3m and our staff is being greatly strengthened.[15]

These comments by Malcolm Rifkind actually go to the heart of the matter in some countries and in at least some instances: 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? In a Georgian context this would mean that the Parliament of Georgia must not only seek to get the law right but also that it should ensure that the Government adequately resources all legally-mandated oversight mechanisms. It is therefore clear that what is actually required in Georgia, as in several other places in 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.

Meanwhile to be sure that the relevance of the UK position is made clear, even in its inadequacies, it is worth noting that barely six months after October 2013 when the Chair of the UK Parliament's Intelligence Committee outlined his perspective as indicated above, in May 2014 "a highly critical report by the Commons home affairs select committee … calls for a radical reform of the current system of oversight of MI5, MI6 and GCHQ, arguing that the current system is so ineffective it is undermining the credibility of the intelligence agencies and parliament itself."[16] In this, the Commons Home Affairs Select Committee was not saying anything terribly new but simply echoing the long-held views of a previous Legal Director of MI5, David Bickford who told the Guardian "Britain's intelligence agencies should seek authority for secret operations from a judge rather than a minister because public unease about their surveillance techniques is at an all-time high. Bickford said the government should pass responsibility to the courts because of widespread "dissatisfaction with the covert, intrusive powers of the UK intelligence and law enforcement agencies". [17]

The moral of the story should be clear: Georgia should avoid the pitfalls highlighted in the UK situation and instead opt for a system of judicial oversight of interception and surveillance, whether carried out by LEAs or SIS, which keeps politicians out of the oversight regime completely. Some brief suggestions on how this could be achieved are given in the summary recommendations below.

Key Issue No 4 – Treat LEAs and SIS differently? In many respects, No

The fourth key issue is one that has been highlighted in a number of previous reports including the most recent Vodafone Law Enforcement Disclosure Report:

> "The protection of national security is a priority for all governments. This is reflected in legislative frameworks which grant additional powers to agencies and authorities

---

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

[16] Travis, A , *MPs: Snowden files are 'embarrassing indictment' of British spying oversight All-party committee demands reforms to make security and intelligence services accountable in wake of disclosures* The Guardian, May 9th 2014 last accessed on 02 September 2014 at http://www.theguardian.com/uk-news/2014/may/09/edward-snowden-mps-commons-report-spying

[17] Hopkins N & Taylor M, *"Cabinet was told nothing about GCHQ spying programmes, says Chris Huhne,"* The Guardian, 6 October 2013 last accessed on 02 September 2014 at http://www.theguardian.com/uk-news/2013/oct/06/cabinet-gchq-surveillance-spying-huhne

engaged in national security matters which typically exceed powers available for domestic law enforcement activities. For example, in many countries, domestic law enforcement legislation seeks to achieve some form of balance between the individual's right to privacy and society's need to prevent and investigate crime. Those considerations have much less weight in the context of threats to the state as a whole, particularly when those threats are linked to foreign nationals in foreign jurisdictions".[18]

To complete the picture it is worth recalling the findings of the PUPIE project[19] which suggests that Security Services 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. Indeed, was there noted that "There is limited agreement on the meaning of 'state security', as it depends on national policies (at national level, the use/application of the phrase 'national security' or 'state security' may be confusing). The majority of countries surveyed applied data protection rules to data processed for state security purposes, while two countries reported such activity is regulated by a specific, separate data protection law."[20]

In the case of Georgia no convincing evidence has been presented that the Georgian LEAs require a less strict legal and oversight regime than the Georgian SIS – or vice-versa - so it is very strongly recommended that "what is good for the goose is good for the gander" and that both LEAs and SIS be subjected to the same oversight regimes and legal provisions offering high standards of protection for data subjects with no discrimination being made between protection for Georgian or non-Georgian nationals.

Summary of key recommendations:

1. Use one or more documents produced by leading service providers such as Vodafone (sample copy attached) to draw up a check-list of the issues to be addressed by the legislation, taking into account those areas which service providers find to be particularly thorny and come up with draft provisions which address each of those issues in a detailed and methodical manner.

2. Use the check-list produced as a result of the first recommendation above as the starting point of the next phases of discussions with service providers, civil society groups and other stakeholders including LEAs and SIS within Georgia. This would provide an invaluable validation exercise on the precise nature of the legislative, technical and administrative safeguards that should be introduced to maximise

[18] Law Enforcement Disclosure Report 2013-2014, published as part of the Vodafone Group plc Sustainability Report, Page 71

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

[20] Ibid at page.11 .

citizen security and confidence in the system as well as the flexibility to respond to the various security threats in an adequate and timely manner.

3. Consolidate the findings of the consultation exercise and produce an advanced draft of the proposed legislative amendments taking the following actions into consideration:
    a. Annul any legislation which enables agencies and authorities to access an operator's communications infrastructure without the knowledge and direct control of the operator,
    b. Provide for a two-key technical solution where the law requires that any technical means of access to a service provider's infrastructure would, to enable access, require a key held by the designated on-duty senior executive of the service provider, which key could only be used legitimately on sight of a properly-issued judicial warrant.
    c. Provide penalties for agencies and authorities seeking direct access to an operator's communications infrastructure without a lawful mandate
    d. Learn from the experience of other countries, including the UK, and, as part of the legislative solution, in order to maximise citizen confidence and minimise the risk of political vested interests getting in the way, create a system of oversight which does not depend on politicians and indeed by-passes them as completely as possible by making lawful interception dependent on judicial oversight requiring warrants to be issued by Judges well-trained for the purpose. (i.e. from a pool of judges well-trained in both data protection law and security issues)
    e. The judicial oversight system should not depend on one judge: the system created should be adequately resourced with a pool of a minimum of five, an average of twenty and, say, a maximum of thirty, judges operating across three 80 hour-shifts who, while competent to carry out a whole range of normal judicial tasks in civil, commercial and/or criminal law, would also be specially trained in privacy and data protection law as well as in security matters (a special curriculum for an intensive immersion course could be easily put together for the purpose and delivered with assistance from the Council of Europe). The police, secret services or prosecutor should not be in a position to know to whom their request for a judicial warrant would be presented: this would be determined by a very confidential computerised roster system which would automatically allocate the decision to issue a warrant to a member of the pool who would be on call for a particular 8 hour shift.
    f. Promote openness, transparency and thus citizen confidence by legislating mandatory publication of lawful interception statistics by the Government using reports from LEAs, SIS and judicial review college and mandatory resourcing of independent audit of such statistics by the national Data Protection Authority of Georgia.