Group Briefing

February 2015

All Leaks, No Flood? Surveillance of Electronic Communications for Intelligence and National Security Purposes

KEY CONTACTS

For further information, please speak to your usual Arthur Cox contact or one of the following:

PEARSE RYAN
PARTNER, TECHNOLOGY & INNOVATION
+353 1 618 0518
pearse.ryan@arthurcox.com

GOLDA HESSION
TRAINEE, TECHNOLOGY & INNOVATION
+353 1 618 0661
golda.hession@arthurcox.com

INTRODUCTION

As the dust begins to settle on the Snowden revelations, public awareness has undoubtedly been focussed on the extent of intelligence surveillance carried out in the name of national security. Our engagement with data presents challenges for citizens, industry and policymakers alike. It is perhaps timely, therefore, to revisit the balance currently struck by the data protection regime in facilitating digital innovation while protecting the privacy rights of individuals. Indeed there has been relatively little change in law and policy since the Snowden leaks in mid-2013.

Of particular interest is the evolving concept of national security, no longer being synonymous with geographic borders, and its impact on the rights and obligations of individuals and organisations as well as the future development of that concept in the digital sphere.

These are the questions that the Article 29 Working Party on the Protection of Individuals with regard to the Processing of Personal Data (the "WP29") is beginning to ask in a series of documents it has authored over the past year.

THE ARTICLE 29 WORKING PARTY

The WP29 was set up under Article 29 of the EU Data Protection Directive 95/46/EC (the "Data Protection Directive"). The WP29 is composed of a representative from the data protection authority of each EU Member State (including the Irish Data Protection Commissioner), the European Data Protection Supervisor and the European Commission. The WP29 has advisory status and acts independently, making non-legally binding recommendations and giving opinions to the Commission on all matters relating to the protection of persons with regard to the processing of personal data in the Union.

Its most recent body of work aims to launch a debate as to the necessary follow-up to the Snowden revelations, in order to *"restore respect for the fundamental rights of privacy and data protection by the intelligence and security services"*, and includes:

» An Opinion on surveillance of electronic communications for intelligence and national security purposes (the "Opinion"); [1]

» A Joint Statement on European values and surveillance for security

1 Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes, WP215, 10 April 2014

purposes (the "Declaration");[2] and

» A Working Document on surveillance of electronic communications for intelligence and national security purposes (the "Working Document").[3]

THE OPINION

In April 2014 the WP29 adopted an Opinion concluding that *"secret, massive and indiscriminate surveillance programs are incompatible with our fundamental laws and cannot be justified by the fight against terrorism or other important threats to national security."*[4] Further, it emphasised that restrictions to the fundamental rights of all citizens could only be accepted if the measure is *"strictly necessary and proportionate in a democratic society."*

The Opinion included a number of recommendations to facilitate respect for the rule of law, including:

» more transparency on how surveillance programmes work, including better information to individuals when access to data has been given to intelligence services. The WP29 considers that such transparency will enhance and restore trust between citizens, governments, and private entities;

» more meaningful oversight of surveillance activities, including on processing of personal data, with genuine involvement of data protection authorities;

» enforcement of existing obligations of EU Member States and parties to the European Convention on Human Rights ("ECHR") to protect the rights of respect for private life and the protection of personal data. In particular, existing agreements with third countries must be interpreted restrictively and cannot legally justify the transfer of personal data to a third country authority "for the purpose of massive and indiscriminate surveillance";

» negotiations at EU and international level on data protection reform in the context of intelligence surveillance; and

» clarification of the scope of the national security exemption to the application of EU law.

THE DECLARATION

The Declaration adopted by WP29 on 25 November 2014 sets out a number of succinct key messages relating to European values, the right to data protection and its place amongst the equal rights of non-discrimination and freedom of expression. The Declaration notes that technical feasibility is not commensurate with data processing that is reasonable, lawful or socially acceptable.

In relation to surveillance for security purposes, the Declaration echoes its earlier Opinion by stating that *"secret, massive and indiscriminate surveillance of individuals"*[5] in Europe and unrestricted bulk retention of data for security purposes, either by public or private bodies, acting in an EU Member State or elsewhere, are not lawful under the EU Treaties, nor are they foreseen by European instruments designed to frame international data transfers. Again, calls for increased oversight of surveillance activities made in the Opinion are reiterated.

The language is certainly emphatic, questioning not only the legality but the ethical and social acceptability of large-scale surveillance. The WP29 invited comments on the Declaration by interested stakeholders, public and private.

THE WORKING DOCUMENT

The Working Document was adopted by the WP29 on 5 December 2014, and contains the result of the discussions and legal analysis on which the Opinion recommendations, published seven months earlier, are based. It seeks to comprehensively analyse the multi-layered legal landscape within which the monitoring and transfer of personal data take place and the Venn diagram of rights, obligations and legal orders that correspond to potential data flows between private actors and intelligence agencies. Filling to the greatest extent possible any potential gaps created by the national security exemption imposed by Article 4(2) of the Treaty on European Union ("TEU") is the overriding thrust of this analysis.

This is no simple task and takes place in the context of the relatively sparse information available as to the existence and operation of surveillance programmes by European governments and third countries, which is largely gleaned from press reports and the work of privacy advocacy groups. While a detailed review of each strand of the legal framework is beyond the scope of this article, it is worth briefly examining the principal elements of the WP29's analysis:

» ***United Nations Legal Instruments***
The Working Document first examines provisions in the realm of international human rights law for privacy protection and emphasises the obligations of states not only to promote respect for human rights but to take necessary steps to give effect to such rights under the Charter of the UN and the International Covenant on Civil and Political Rights (the "Covenant").[6] The Working Document draws attention to the UN General Assembly resolution of January 2014[7] reaffirming the Covenant's rights and calling upon State parties to establish independent national oversight mechanisms to ensure transparency and accountability of State surveillance of communications and the interception and collection of personal data. The Resolution acknowledges the balance to be struck

2 Joint Statement of the European Data Protection Authorities assembled in the Article 29 Working Party, WP 227, 26 November 2014

3 Working Document on surveillance of electronic communications for intelligence and national security purposes, WP228, 5 December 2014

4 Opinion, at p. 1

5 Declaration at p. 3

6 Article 12 of the Universal Declaration of Human Rights and Article 17 of the Covenant declare than no one shall be subjected to arbitrary or unlawful interference with his privacy

7 UN General Assembly Resolution 68/167, 21 January 2014

between privacy and security but affirms that individuals have the same rights online as offline and must be protected across all digital platforms.

The Working Document also details the work of the UN High Commissioner for Human Rights in his recent report on the Right to Privacy in the Digital Age. The timely report gives context to the WP29's current work, calling on states to immediately review their own national laws and policies to ensure full conformity with international human rights law and the "clear and pressing need for vigilance" in ensuring effective safeguards in surveillance policy.[8]

» ***Council of Europe Instruments***

The Working Document goes on to examine the obligations of European states under Article 8 of the ECHR (right to respect for private life), to which all 28 EU Member States are subject, and the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention 108").

The scope of application of ECHR law is a crucial part of the applicable legal landscape as, while it incorporates various security-related derogations from individual rights, there is no general national security exemption to its scope as in the case of the TEU. The ECHR boasts a significantly more advanced body of law in the area of privacy than the UN and its judicial oversight is recognised by the EU as offering an equivalent level of protection to the EU regime. Its membership is wider, including Russia, Ukraine and the Balkans, and its jurisdiction extends to all individuals within the jurisdiction, regardless of nationality or place of residence.

The Working Document cites jurisprudence of the European Court of Human Rights ("ECtHR") to the effect that any permitted derogations under Article 8(2) in the name of national security, public safety, the prevention of disorder or crime or the protection of the rights and freedoms of others, must be narrowly interpreted and confined to what is strictly necessary in a democratic society. Measures are necessary when they answer a pressing social need, are proportionate to the aim and justified by relevant and sufficient reasons put forward by the relevant public authority.

As far back as 1978, the ECtHR specified that *"powers of secret surveillance of citizens, characterising as they do the police state, are tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions."*[9]

» ***European Union Law***

The bulk of the Working Document is dedicated to analysing the various EU instruments that have a bearing on data protection, from the EU Charter of Fundamental Rights (the "Charter"), the Data Protection Directive, the e-Privacy Directive[10], and the transfer regime governed by the Safe Harbor Agreement, Standard Contractual Clauses and Binding Corporate Rules.
Crucial to this analysis however, and as mentioned above, is the national security exemption from the scope of EU law (including the Charter) contained in Article 4(2) TEU, which recognises that *"national security remains the sole responsibility of each Member State"*. Relatively little investigation has been carried out into the definition and scope of the concept of national security, given that this is the premise upon which intelligence and security services are generally assumed to carry out their tasks. The impact of the exemption is that EU institutions are not competent to act, either to legislate or review, with regard to matters of national security.

THE RELATIONSHIP BETWEEN NATIONAL SECURITY AND DATA PROTECTION

The WP29 deals with matters which are by their nature inherently complex. The Opinion Declaration and Working Document are amongst the (if not the) most complex documentation yet produced and likely deal with the area least generally understood by politicians, populace and lawyers alike. The Working Document goes on to assess perhaps the most complex of areas in some detail, namely, the interaction between data protection and national security, under a number of headings:

» ***Concept of National Security***

So "national security" is carved-out, but what of analogous or closely connected concepts contained in the EU Treaties where the Union is competent to legislate?

The obvious example is the legal basis provided in the Treaty on the Functioning of the EU ("TFEU") under the Area of Freedom, Security & Justice to legislate, to prevent and to combat terrorism and related crime, a clear overlap with national security. The Terrorist Finance Tracking Program for example sees Member States, the EU and the US cooperate closely by sharing financial transaction information for security purposes and is subject to rules agreed at EU level.

Likewise the concept of "Union security" comes within the EU's bailiwick under the Common Foreign & Security Policy. The E-Commerce Directive[11], the Data Protection Directive and others refer to derogations in the name of "public security, defence [and] State security".

It is hard to argue with the WP29's view that these concepts are inextricably linked and the functional reality of the national security exemption has been driven by political imperative where cooperation at Union level has been desired (or not). And what of

8 Opinion, p. 13

9 *Klass and others v Germany* (1978) 2 EHRR 214, para. 42

10 Directive 2002/58/EC

11 Directive 2000/31/EC

activities carried out by general law enforcement authorities rather than intelligence services; does the actor have a role in whether national security is at issue?

The Working Document concludes that only the Court of Justice of the EU ("CJEU") is competent to define the scope of Union law and concepts forming part of the treaties. It has already developed jurisprudence in the area of counter-terrorism to the effect that the obligations of an international agreement cannot prejudice the principles of the EU treaties, including respect for fundamental rights. [12]

» ***National Security of Third Countries***

The WP29 is adamant however that the national security exemption applies only to the relationship between Member States and the EU vis-à-vis the sovereignty to act, and does not negate any obligation to comply with EU data protection requirements on foot of requests by third countries in the name of their national security. The Working Document also points out the dissonance between national security and the purposes for which third countries permit themselves to carry out surveillance, such as the terms of the US Foreign Intelligence Surveillance Act 1978 ("FISA"). Matters are complicated further by a scenario where the national security of a third country coincides with the national security of a Member State, thereby falling inside the national security exemption from EU law.

» ***EU Data Protection Regime***

The Working Document points out the continued relevance of the Data Protection Directive where data controllers and processors are ordered to submit information to intelligence and law enforcement services (rather than the regulation of data processing by intelligence agencies themselves) or transfers for commercial purposes between private parties. The WP29 refers to its own guidelines as to the territorial scope of application of the Directive, e.g. the use of equipment situated in the EU by non EU-established data controllers. Any exercise of derogations in the name of security or defence foreseen by the Directive must be laid down in Member States' laws with appropriate safeguards.

» ***Data Transfers***

With regard to data transfers to third countries recognised as having an adequate level of data protection, the Working Document recalls that the level of adequacy recognised in the Safe Harbor Agreement is in the context of commercial data transfers. The WP29 argues that Safe Harbor was not designed to offer adequate levels of protection for law enforcement or other purposes in contrast, for example, to the Passenger Name Records (PNR) Agreements which were designed for law enforcement and counter-terrorism purposes. The Working Document recognises the work undertaken by the European Commission to address reforms to Safe Harbor in recognition of the large scale access by intelligence agencies to personal data transferred to the US, and goes so far as to call for the suspension of the agreement if the Commission revision process does not *"lead to a positive outcome"*.[13] The Working Document acknowledges that different legal regimes will apply to data transfers depending on whether they are intra- or extra-EU, between public or private entities, for the purposes of national security, law enforcement or otherwise. The potential scenarios are myriad and present obvious compliance difficulties.

» ***Looking forward – options for reform***

The Working Document points to the ongoing negotiation of the new General Data Protection Regulation[14] and a proposal to introduce a new Article 43a made by the European Parliament's Civil Liberties, Justice and Home Affairs Committee. The Article relates to transfers or disclosures not authorised by Union law and recalls that disclosure of personal data to any authority of a third country should only take place after notification of the request and prior authorisation of the supervisory authority, without prejudice to any Mutual Legal Assistance Treaty or other international agreement in force between the requesting third country and the Member State or the EU. Any authorisation by a supervisory authority to grant a request must be based on an assessment of compliance with the Data Protection Regulation. The request should also be notified to the competent national law enforcement authority and certain information disclosed to data subjects.

The Working Document concludes however that, while helpful, the proposed Article 43a will not solve all open legal questions, such as the concepts of *"national security"* and *"data transfers"*.

CONCLUSION

The detailed work of the WP29 in both a politically sensitive and legally complex area is to be welcomed, particularly in light of its stated aim to launch a debate on the role of EU law in protecting fundamental rights in the face of large-scale surveillance by intelligence agencies operating in furtherance of their national security.

This debate has escalated in immediacy since the publication of the Working Document due to the Charlie Hebdo and Sydney attacks. The intelligence

12 Working Document, p. 24

13 Working Document, p. 41

14 COM(2012) 11 final

community is calling for increased access to encrypted email, Skype calls and messaging services to combat the threat of further terrorist attacks.[15] In the context of the current Microsoft litigation concerning intelligence services seeking access to emails stored in the cloud, privacy campaigners such as Caspar Bowden highlight the breadth of legal instruments under which information can currently be sought by US authorities outside Safe Harbor and binding corporate rules. Bowden has pointed out the risks this entails for cloud customers of US firms, especially where stored data is processed, rather than remaining encrypted. He argues that companies need to take more responsibility in their selection of cloud providers to minimise the opportunities for surveillance.[16]

The nexus between the many layers that constitute the data protection regime, current and future risk for commercial data controllers and processors, and the legitimate goals of guaranteeing public safety is crystallising. The dust is far from settled on the post-Snowden era. A flood may yet follow the leaks.

15 Hennesy, Mark, "Spy services must be able to tap emails, say ex-MI6 chief", The Irish Times, 20 January 2015

16 Leonard, John, "Privacy campaigner: Why I hope Microsoft loses court case against the NSA", Computing, 13 January 2015