CEPS COMMENTARY
Thinking ahead for Europe

Who will monitor the spies?

Sergio Carrera, Elspeth Guild and Joanna Parkin

8 January 2014

On 26 September 2013, the European Parliament invited Sir Iain Lobban, Director of the UK's intelligence-gathering agency GCHQ, to testify before the LIBE Committee inquiry on the electronic surveillance of EU citizens.[1] MEPs wanted answers in the face of mounting evidence (obtained from leaks by former NSA contractor Edward Snowden) of the UK's involvement in wide-ranging and illegal surveillance practices linked to the NSA-led PRISM programme, including the routine mass interception of communications data and cyber-hacking of foreign companies and diplomats. In declining the Parliament's invitation, the UK government was unequivocal: "National security is the sole responsibility of Member States. The activities of intelligence services are equally the sole responsibility of each Member State and fall outside the competence of the Union."

This view, echoed by the EU's former Lithuanian Presidency as justification for limiting EU-US discussions that followed the Snowden disclosures,[2] is largely shared by the member states. A majority of national governments across the EU have long tried to ring-fence matters of national security from supranational scrutiny by the EU institutions and courts by arguing that these remain within the remit of their 'exclusive competence'. Yet in light of the revelations indicating that more EU member states (namely Sweden, France and Germany) are running their own secret interception programmes (albeit on a smaller scale),[3] the question of whether the EU can and should intervene becomes more pressing. Are the covert, large-scale surveillance programmes of member states beyond the scope of EU intervention? This commentary puts forward four important legal reasons why the answer to this question should be no.

[1] The European Parliament's Inquiry on the Electronic Mass Surveillance of EU Citizens was launched in July 2013, following the revelations of Edward Snowden and ran until December 2013.

[2] Letter of Dalia Grybauskaitė, President of Lithuania to Martin Schulz, President of the European Parliament of 30 July 2013 (http://www.europarl.europa.eu/meetdocs/2009_2014/organes/libe/libe_20130912_1000.htm).

[3] These allegations and their implications for EU law are explored in more detail in the CEPS study by D. Bigo et al. (2013), "Mass Surveillance of Personal Data by EU Member States and its Compatibility with EU Law", CEPS Paper in Liberty and Security in Europe No. 61, CEPS, Brussels, November.

Sergio Carrera is Senior Research Fellow and Head of the Justice and Home Affairs research programme at CEPS. Elspeth Guild is Senior Associate Research Fellow in the Justice and Home Affairs research programme at CEPS, Jean Monnet Professor ad personam of European Migration Law at the Radboud University Nijmegen, the Netherlands, and Queen Mary, University of London. Joanna Parkin is a Researcher, Justice and Home Affairs section, CEPS.

First, the EU is competent to regulate and protect the fundamental rights of data protection and privacy, and any derogation member states wish to apply to those rights must be overseen by European institutions and courts. The EU's competence over data protection is regulated by a raft of data protection directives, which are currently being updated and extended under the so-called 'data protection reform package'. Furthermore, the EU is charged with protecting the privacy rights of Union citizens and the privacy of everyone falling within the scope of EU law, as enshrined in the EU Charter of Fundamental Rights. Any interference with privacy rights and data protection obligations – and the large-scale surveillance of an individual's communications data cannot constitute anything but – must be justified under EU law.

National security is one of the grounds available to state authorities to justify interference with the exercise of an EU protected right. However, any limitation of a fundamental right, including on grounds of national security, must be interpreted restrictively, according to the Court of Justice of the EU (CJEU).[4] It is ultimately for the CJEU to ensure that this interference does not go beyond what is permitted by law, that it is proportionate to a legitimate aim and limited to what is necessary in a democratic society to achieve that aim. Thus, while it is in the first instance the prerogative of member states to assess their own national security needs, when that assessment results in the interference with an EU right, then the compatibility of the national security measure is a matter to be determined by the EU institutions.

Second, secret surveillance is not only subject to EU oversight, but it also falls under strict judicial control by the European Court of Human Rights. It is highly uncertain that the large-scale surveillance as alleged to be practiced by the UK and others would be deemed lawful within the judicial system governed by the European Convention on Human Rights. In its jurisprudence the Strasbourg court has established detailed criteria with which to determine the legality of a state's secret interception of communications. According to the Court, surveillance should be targeted, and domestic law regulating surveillance must be "foreseeable": in other words, formulated with sufficient precision so as to guarantee legal certainty. This is a critical condition to prevent the arbitrary and unfettered use of powers by security agencies. The court's firm position on surveillance was recently supported at international level by the UN resolution of 18 December 2013, which recognises an international right to privacy and calls on governments to respect and protect this international right.[5] We doubt that the mass, routine and indiscriminate surveillance as practiced in the UK and elsewhere would meet the Court's minimum standards, nor would they respect these international principles.

Third, to what extent can we distinguish these practices from acts of cybercrime? The Council of Europe's 2001 Convention on Cybercrime identifies illegal access and illegal interception as an offence against the confidentiality, integrity and availability of computer data and systems under criminal law. The EU has taken the Council of Europe Convention as a legal reference point, and building on this foundation is developing a substantial body of policy to boost cybersecurity and enhance its operational capacities with the establishment of the

[4] See C-300/11 Z.Z. CJEU 4 June 2013 and C-293/12 Digital Rights Ireland v Ireland, Opinion of AG Cruz Villalon; see also S. Peers (1996), "National Security and European Law", *Yearbook of European Law*, Vol. 16, No. 1, pp. 363-404.

[5] UN General Assembly draft Resolution on the right to privacy in the digital age, 68th session, Third Committee, 13-54407.

European Cybercrime Centre within the EU's law enforcement agency Europol. Responding to the links made between cybercrime and unlawful state surveillance, Europol Director Rob Wainwright claimed that while the EU's law enforcement agency has a duty to investigate cybercrime at the request of member states, Europol does not have the mandate to investigate cybercrime *by* those member states.[6] Such a statement stands in tension with the Council of Europe Convention, which does not expressly exclude the actions of governments when those actions are unlawful.

Fourth, member states' large-scale surveillance practices blur the lines between national security and matters relating to EU competence when they threaten to spill over into the security activities of the EU institutions and its agencies. Member states may have the main competence in relation to national security, but the Union has shared competence with the member states when it comes to the Union's internal security, particularly as regards the policy areas of terrorism and crime. Indeed there are considerable overlaps between national security and EU internal security. EU security agencies such as Europol, for instance, have been established with the prime task of gathering, exchanging and processing information on 'threats' facing the Union, based on data supplied by the member states' law enforcement and security agencies. The minimal oversight of this information exchange leaves EU agencies unable to verify the original source of the information received, nor guarantee that it has been obtained via lawful means. This becomes particularly problematic should the EU's institutions and its agencies become implicated in using, sharing and exploiting data generated by unlawful surveillance practices, which could leave the EU complicit and potentially liable for any breach of human rights or rule of law standards. Measures enacted under the banner of national security will quite rightly invoke EU interest when those actions jeopardise the internal security of the Union as a whole and make it more difficult for the EU to perform its responsibilities under the treaties in a consistent and coherent fashion.

These four arguments give the EU clear competence to intervene in the wake of the Snowden surveillance scandals. They lend support to the conclusion of the European Parliament inquiry that "discussion and action at EU level is not only legitimate, but also a matter of EU autonomy and sovereignty."[7] The draft report emanating from the Parliament's inquiry has just been published and will be presented to the LIBE Committee on 9 January 2014. It contains a number of important findings and some welcome recommendations that could provide a springboard for the next European Parliament and Commission to take strong follow-up action.

The EU institutions should begin by turning attention to the deficiencies in domestic and European-level oversight of security agencies, in order to remedy the problems of independence and weak technical capacities identified in oversight bodies across EU member states. It would be critical to explore the scope for a European policy infrastructure to provide a permanent oversight mechanism capable of reacting to recurrent breaches by EU and foreign intelligence agencies when they encroach on the rights and freedoms of EU citizens. The European Parliament draft report suggests establishing a 'High Level Group' to develop common standards and strengthen oversight of intelligence bodies, although it doesn't specify which institutional actors would steer such a group or who would ensure the

[6] Testimony of Rob Wainwright at the LIBE Committee Hearing on the Electronic Mass Surveillance of EU Citizens, European Parliament, 24 September 2013.

[7] Draft report of the European Parliament on the Electronic Mass Surveillance of EU Citizens, 2013/2188(INI), 23 December 2013.

implementation of these standards. The danger here of creating another opaque, member state-led task force is all too real.

A more promising approach, potentially delivering more effective democratic scrutiny, would be to embed this oversight mechanism within the European Parliament, by transforming the European Parliament's temporary inquiry into a permanent (joint) parliamentary oversight unit within the LIBE Committee.[8] Composed of a group of LIBE representatives, the proposed unit would focus on the central task of developing an EU professional code for the transnational management of data and intelligence cooperation.[9] The unit would also work closely with national parliaments and could provide a supranational forum for national oversight mechanisms and bodies to meet regularly, thereby addressing current oversight gaps and the lack of resources in domestic arenas. Based on the minimum standards set by the European courts and international instruments, this code could serve as a guiding framework for intelligence bodies and EU agencies, setting the 'red lines' that security bodies cannot cross in democratic regimes when conducting surveillance. [10]

The establishment of an effective European level of oversight would undoubtedly represent a step change in the EU's approach to member states' intelligence activities. Yet, supranational monitoring may be the only way forward now that the evolution in communications technologies has brought about a reconfiguration in surveillance, allowing intelligence communities to access and process personal data on an unprecedented scale. Routine, unauthorised and mass capture of data for strategic surveillance has taken us beyond the traditional post 9/11 debate about the balance between 'security versus privacy'. It puts the very nature of open societies and democratic rule of law at risk and constitutes a systematic and persistent breach of the Union's values; if the EU is seen as ineffective in protecting those principles and its citizens, its very credibility will be called into question.

[8] The EP Draft Report makes reference to "the establishment of a standing oversight mechanism for data transfers and judicial remedies within the competent committee", ibid., p.33.

[9] Other competences could include the close scrutiny and monitoring of EU security agencies, such as Europol. See European Parliament, Draft Report, on the proposal for a regulation of the European Parliament and of the Council on the European Union Agency for Law Enforcement Cooperation and Training (Europol) and repealing Decisions 009/371/JHA and 005/681/JHA, 19.6.2013, Rapporteur: Díaz de Mera.

[10] For a comprehensive set of policy recommendations, see Bigo et al. (2013), op. cit.