Letter to *The Guardian*, Tuesday, 15 March 2016

Dear Editor,

The Investigatory Powers Bill receives its second reading today. At present the draft law fails to meet international standards for surveillance powers. It requires significant revisions to do so.

First, a law that gives public authorities generalised access to electronic communications contents compromises the essence of the fundamental right to privacy and may be illegal. The Investigatory Powers Bill does this with its "bulk interception warrants" and "bulk equipment interference warrants".

Second, international standards require that interception authorisations identify a specific target – a person or premises – for surveillance. The Investigatory Powers Bill also fails this standard because it allows "targeted interception warrants" to apply to groups of persons, organisations, or premises.

Third, those who authorise interceptions should be able to verify a "reasonable suspicion" on the basis of a factual case. The Investigatory Powers Bill does not mention "reasonable suspicion" – or even suspects – and there is no need to demonstrate criminal involvement or a threat to national security.

These are international standards found in the recent opinion of the UN Special Rapporteur for the Right to Privacy, and in judgments of the EU Court of Justice and the European Court of Human Rights. At present the Bill fails to meet these standards – the law is unfit for purpose.

If the law is not fit for purpose, unnecessary and expensive litigation will follow, and further reform will be required. We urge members of the Commons and the Lords to ensure that the future Investigatory Powers Act meets these international standards.

Yours,

Stephen Sedley, **Professor Sir Geoffrey Bindman QC (Hon)**, Solicitor, **Kirsty Brimelow QC**, Barrister, **Tom de la Mare QC**, Barrister, **Stephen Grosz QC (Hon)**, Solicitor, **John Hendy QC**, Barrister, **Stephen Kamlish QC**, Barrister, **Michael Mansfield QC**, Barrister, **Patrick O'Connor QC**, Barrister, **Professor Phillipe Sands QC**, Barrister, **Hugh Southey QC**, Barrister, **Rebecca Trowler QC**, Barrister, **Martin Westgate QC**, Barrister, **Heather Williams QC**, Barrister, **James Wood QC**, Barrister, **Professor Tanya Aplin**, King's College London, **Professor Ben Bowling**, King's College London, **Professor Bill Bowring**, Birkbeck College, **Professor Paul Craig**, University of Oxford, **Professor Fiona de Londras**, University of Birmingham, **Professor Jonathan Doak**, Nottingham Trent University, **Professor Sionaidh Douglas-Scott**, Queen Mary University of London, **Professor Lillian Edwards**, University of Strathclyde, **Professor Piet Eeckhout**, University College London, **Professor Keith D. Ewing**, King's College London, **Professor Helen Fenwick**, University of Durham, **Professor Elspeth Guild**, Queen Mary University of London, **Professor Colin Harvey**, Queen's University Belfast, **Professor Eric Heinze,** Queen Mary University of London, **Professor Kevin Jon Heller,** School of Oriental and African Studies, **Professor Christian Henderson,** University of Sussex, **Professor Tamara Hervey,** University of Sheffield, **Professor Paddy Ireland,** University of Bristol, **Professor Satvinder Juss,** King's College London, **Professor Urfan Kaliq,** Cardiff University, **Professor Douwe Korff,** London Metropolitan University, **Professor Aileen McColgan,** King's College London, **Professor Kieran McEvoy,** Queen's University Belfast, **Professor Valsamis Mitsilegas,** Queen Mary University of London, **Professor Andrew Murray,** London School of Economics, **Professor Mike Nellis,** University of Strathclyde, **Professor Colm O Cinnéide,** University College London, **Professor Rory O'Connell,** Ulster University, **Professor Laurent Pech,** Middlesex University, **Professor Steven J. Peers,** University of Essex, **Professor Gavin**

Phillipson, University of Durham, **Professor Daniel Wilsher,** City University London, **Dr Diego Acosta Arcarazo,** University of Bristol, **Dr Abayomi Al-Ameen,** Cardiff University, **Dr Gavin W. Anderson,** University of Glasgow, **Aamer Anwar,** Solicitor, **Nick Armstrong,** Barrister, **Rodney Austin,** University College London, **Dr Kimberley Barker,** University of Wolverhampton, **Dr Ed Bates,** University of Leicester, **Gunnar Beck,** Barrister, **Dr Paul Bernal,** University of East Anglia, **Dr Stephanie E. Berry,** University of Sussex, **Dr Jessie Blackbourn,** Kingston University, **Nicholas Bohm,** Solicitor, **Brian Brazier,** Paralegal, **Nick Brown,** Barrister, **Jude Bunting,** Barrister, **Dr Christine Byron,** Cardiff University, **Brenda Campbell,** Barrister, **Dr Liz Campbell,** University of Edinburgh, **Grace Capel,** Barrister, **Jules Carey,** Solicitor, **Daniel Carey,** Solicitor, **David Carter,** Barrister, **Dr Theodora Christou,** Queen Mary University of London, **Paul Clark,** Barrister, **Gerard Clarke,** Barrister, **Deborah Coles,** Solicitor, **Jonathan Cooper,** Barrister, **Dr Nicola Countouris,** University College London, **Caroline E. Cross,** Barrister, **Daniele D'Alvia,** Birkbeck College, **Dr Fergal Davis,** King's College London, **Dr Hazel Dawe,** Birkbeck College, **Jane Deighton,** Solicitor, **Kevin Donoghue,** Solicitor, **Laura Dubinsky,** Barrister, **Jim Duffy,** Barrister, **Dr Kanstantin Dzehtsiarou,** University of Liverpool, **Matthew Evans,** Solicitor, **Dr Elaine Fahey,** City University London, **Sarah Flanagan,** Solicitor, **Dr Tom Flynn,** University of Warwick, **Eleni Frantziou,** University of Westminster, **Dr Tom Frost,** University of Sussex, **Caoilfhionn Gallagher,** Barrister, **Dr Amadine Garde,** University of Liverpool, **Dr Sabrina Gilani,** University of Sussex, **Matthew Gold,** Solicitor, **Dr Andrew Green,** University of Sheffield, **Graeme Hall,** Barrister, **Alice Hardy,** Solicitor, **Charlotte Haworth Hird,** Solicitor, **Dr David J. Hayes,** University of Sheffield, **Rory Hearty,** Solicitor, **William Henderson**, Glasgow Caledonian University, **Leonie Hirst,** Barrister, **Dr Hayley J. Hooper**, University of Cambridge, **Dr Kirsty Hughes**, University of Cambridge, **Adam Hundt**, Solicitor, **Dr Adrian Hunt**, University of Birmingham, **Myles Jackson**, Solicitor, **Harriet Johnson**, Barrister, **Tom Jones**, Solicitor, **Rhiannon Jones**, Assistant Solicitor, **Mikhil Karnik**, Barrister, **Andrew Katz**, Solicitor, **Dr David Keane**, Middlesex University, **Bernard Keenan**, London School of Economics, **Perry Keller**, King's College London, **Arthur Kendrick**, Paralegal, **Imran Khan**, Solicitor, **Eric King,** Queen Mary University of London, **Maya Lal,** Solicitor, **Kumari Lane,** Birkbeck College, **Dr Liora Lazarus,** University of Oxford, **Mark Leiser,** University of Strathclyde, **Dr Genevieve Lennon,** University of Strathclyde, **Rachel Logan,** Barrister, **Darragh Mackin,** Solicitor, **Dr Bharat Malkani,** University of Birmingham, **Christopher Markou,** University of Cambridge, **Estelle Marks,** King's College London, **Amber Marks,** Queen Mary University of London, **Charles Marquand,** Barrister, **Dr Natasa Mavronicola,** Queen's University Belfast, **Dr Padraig McAuliffe,** University of Liverpool, **Dr Christopher McCorkindale,** University of Strathclyde, **Conor McCormick,** Queen's University Belfast, **Dr Yvonne McDermott Rees,** Bangor University, **Victoria McEvedy,** Solicitor, **Simon McKay,** Barrister, **Dr Nick McKerrell,** Glasgow Caledonian University, **Gráinne Mellon,** Barrister, **Eric Metcalfe,** Barrister, **Roy Mincoff,** Solicitor, **Helen Mowatt,** Trainee Solicitor, **Dr Jo Muerkens,** London School of Economics, **Dr Stephen J. Murdoch,** University College London, **Tony Murphy,** Solicitor, **Dr Cian Murphy,** King's College London, **Colin Murray,** Newcastle University, **Charles Myers,** Solicitor, **Ravi Naik,** Solicitor, **Dr Eva Nanopoulos,** University of Cambridge, **Omar Naqib,** Solicitor, **Subashini Nathan,** Barrister, **Dr Bríd Ní Ghráinne,** University of Sheffield, **Dr Nora Ni Loideain,** University of Cambridge, **Jesse Nicholls,** Barrister, **Carly Nyst,** Independent, **Greg O Ceallaigh,** Barrister, **Maria O'Connell,** Solicitor, **Aidan O'Donnell,** University of Strathclyde, **Dr Noreen O'Meara,** University of Surrey, **Gillian Phillips,** Solicitor, **Dr Eva Pils,** King's College London, **Dr Julia Powles,** University of Cambridge, **Jonathan Price,** Barrister, **Dr Tara Lai Quinlan,** University

of Sheffield, **Ali Raiss-Tousi,** Birkbeck College, **Paul Ridge,** Solicitor, **Jaani Riordan,** Barrister, **Patrick Roche,** Barrister, **Deborah Russo,** Solicitor, **Adam Sandell,** Barrister, **Joseph Savirimuthu,** University of Liverpool, **Anton Schutz,** Birkbeck College, **Dr Kirsteen Shields,** University of Dundee, **Bethany Shiner,** Solicitor, **Gus Silverman,** Solicitor, **Natasha Simonsen,** King's College London, **Kemi Spector,** Solicitor, **Martha Spurrier,** Barrister, **Alison Stanley,** Solicitor, **Angela Stevens,** Solicitor, **Dr Sujitha Subramanian,** University of Bristol, **Samantha Taylor,** Paralegal, **Gwawr Thomas,** Barrister, **Anna Thwaites,** Solicitor, **Chris Topping,** Solicitor, **Dr Maria Tzanou,** Keele University, **Anthony Vaughan,** Barrister, **Dr Asma Vranaki,** University of Oxford, **John Wadham,** Solicitor, **Adam Wagner,** Barrister, **Amos Waldman,** Barrister, **Liam Walker,** Barrister, **Tony Ward,** University of Hull, **Camille Warren,** Barrister, **Sue Willman,** Solicitor, **Dr Maggie Wykes,** University of Sheffield, **Adrienne Yong,** University of Hertfordshire, **Dr Alison Young,** University of Oxford, **Dr Hakeem O. Yusuf,** University of Birmingham, **Dr Aldo Zammit Borda,** Anglia Ruskin University, **Dr Reuven Ziegler,** University of Reading.

Court of Justice of the European Union
PRESS RELEASE No 117/15
Luxembourg, 6 October 2015

Press and Information

Judgment in Case C-362/14
Maximillian Schrems v Data Protection Commissioner

The Court of Justice declares that the Commission's US Safe Harbour Decision is invalid

Whilst the Court of Justice alone has jurisdiction to declare an EU act invalid, where a claim is lodged with the national supervisory authorities they may, even where the Commission has adopted a decision finding that a third country affords an adequate level of protection of personal data, examine whether the transfer of a person's data to the third country complies with the requirements of the EU legislation on the protection of that data and, in the same way as the person concerned, bring the matter before the national courts, in order that the national courts make a reference for a preliminary ruling for the purpose of examination of that decision's validity

The Data Protection Directive[1] provides that the transfer of personal data to a third country may, in principle, take place only if that third country ensures an adequate level of protection of the data. The directive also provides that the Commission may find that a third country ensures an adequate level of protection by reason of its domestic law or its international commitments. Finally, the directive provides that each Member State is to designate one or more public authorities responsible for monitoring the application within its territory of the national provisions adopted on the basis of the directive ('national supervisory authorities').

Maximillian Schrems, an Austrian citizen, has been a Facebook user since 2008. As is the case with other subscribers residing in the EU, some or all of the data provided by Mr Schrems to Facebook is transferred from Facebook's Irish subsidiary to servers located in the United States, where it is processed. Mr Schrems lodged a complaint with the Irish supervisory authority (the Data Protection Commissioner), taking the view that, in the light of the revelations made in 2013 by Edward Snowden concerning the activities of the United States intelligence services (in particular the National Security Agency ('the NSA')), the law and practice of the United States do not offer sufficient protection against surveillance by the public authorities of the data transferred to that country. The Irish authority rejected the complaint, on the ground, in particular, that in a decision of 26 July 2000[2] the Commission considered that, under the 'safe harbour' scheme,[3] the United States ensures an adequate level of protection of the personal data transferred (the Safe Harbour Decision).

The High Court of Ireland, before which the case has been brought, wishes to ascertain whether that Commission decision has the effect of preventing a national supervisory authority from investigating a complaint alleging that the third country does not ensure an adequate level of protection and, where appropriate, from suspending the contested transfer of data.

In today's judgment, the Court of Justice holds that **the existence of a Commission decision** finding that a third country ensures an adequate level of protection of the personal data transferred **cannot eliminate or even reduce the powers available to the national supervisory authorities**

[1] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31).
[2] Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (OJ 2000 L 215, p. 7).
[3] The safe harbour scheme includes a series of principles concerning the protection of personal data to which United States undertakings may subscribe voluntarily.

under the Charter of Fundamental Rights of the European Union and the directive. The Court stresses in this regard the right, guaranteed by the Charter, to the protection of personal data and the task with which the national supervisory authorities are entrusted under the Charter.

The Court states, first of all, that no provision of the directive prevents oversight by the national supervisory authorities of transfers of personal data to third countries which have been the subject of a Commission decision. Thus, **even if the Commission has adopted a decision, the national supervisory authorities**, when dealing with a claim, **must be able to examine, with complete independence, whether the transfer of a person's data to a third country complies with the requirements laid down by the directive**. Nevertheless, the Court points out that it alone has jurisdiction to declare that an EU act, such as a Commission decision, is invalid. Consequently, where a national authority or the person who has brought the matter before the national authority considers that a Commission decision is invalid, that authority or person must be able to bring proceedings before the national courts so that they may refer the case to the Court of Justice if they too have doubts as to the validity of the Commission decision. **It is thus ultimately the Court of Justice which has the task of deciding whether or not a Commission decision is valid.**

The Court then investigates whether the Safe Harbour Decision is invalid. In this connection, the Court states that the Commission was required to find that the United States in fact ensures, by reason of its domestic law or its international commitments, a level of protection of fundamental rights essentially equivalent to that guaranteed within the EU under the directive read in the light of the Charter. The Court observes that the Commission did not make such a finding, but merely examined the safe harbour scheme.

Without needing to establish whether that scheme ensures a level of protection essentially equivalent to that guaranteed within the EU, the Court observes that the scheme is applicable solely to the United States undertakings which adhere to it, and United States public authorities are not themselves subject to it. Furthermore, national security, public interest and law enforcement requirements of the United States prevail over the safe harbour scheme, so that United States undertakings are bound **to disregard, without limitation, the protective rules laid down by that scheme where they conflict with such requirements**. The United States safe harbour scheme thus enables interference, by United States public authorities, with the fundamental rights of persons, and the Commission decision does not refer either to the existence, in the United States, of rules intended to limit any such interference or to the existence of effective legal protection against the interference.

The Court considers that that analysis of the scheme is borne out by two Commission communications,[4] according to which the United States authorities were able to access the personal data transferred from the Member States to the United States and process it in a way incompatible, in particular, with the purposes for which it was transferred, beyond what was strictly necessary and proportionate to the protection of national security. Also, the Commission noted that the persons concerned had no administrative or judicial means of redress enabling, in particular, the data relating to them to be accessed and, as the case may be, rectified or erased.

As regards a level of protection essentially equivalent to the fundamental rights and freedoms guaranteed within the EU, the Court finds **that, under EU law, legislation is not limited to what is strictly necessary where it authorises, on a generalised basis, storage of all the personal data of all the persons** whose data is transferred from the EU to the United States **without any differentiation, limitation or exception being made** in the light of the objective pursued and without an objective criterion being laid down for determining the limits of the access of the public authorities to the data and of its subsequent use. The Court adds that legislation permitting the public authorities to have access on a generalised basis to the content of electronic

[4] Communication from the Commission to the European Parliament and the Council entitled 'Rebuilding Trust in EU-US Data Flows' (COM(2013) 846 final, 27 November 2013) and Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU (COM(2013) 847 final, 27 November 2013).

communications must be regarded as **compromising the essence of the fundamental right to respect for private life**.

Likewise, the Court observes that legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, **compromises the essence of the fundamental right to effective judicial protection**, the existence of such a possibility being inherent in the existence of **the rule of law**.

Finally, the Court finds that the Safe Harbour Decision denies the national supervisory authorities their powers where a person calls into question whether the decision is compatible with the protection of the privacy and of the fundamental rights and freedoms of individuals. The Court holds that **the Commission did not have competence to restrict the national supervisory authorities' powers in that way**.

For all those reasons, the Court declares the Safe Harbour Decision **invalid. This judgment has the consequence that the Irish supervisory authority is required to examine Mr Schrems' complaint with all due diligence and, at the conclusion of its investigation, is to decide whether, pursuant to the directive, transfer of the data of Facebook's European subscribers to the United States should be suspended on the ground that that country does not afford an adequate level of protection of personal data.**

NOTE: A reference for a preliminary ruling allows the courts and tribunals of the Member States, in disputes which have been brought before them, to refer questions to the Court of Justice about the interpretation of European Union law or the validity of a European Union act. The Court of Justice does not decide the dispute itself. It is for the national court or tribunal to dispose of the case in accordance with the Court's decision, which is similarly binding on other national courts or tribunals before which a similar issue is raised.

Press contact: Christopher Fretwell ☎ (+352) 4303 3355

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

Press Release
issued by the Registrar of the Court

ECHR 382 (2015)
04.12.2015

Arbitrary and abusive secret surveillance of mobile telephone communications in Russia

In today's **Grand Chamber** judgment[1] in the case of Roman Zakharov v. Russia (application no. 47143/06) the European Court of Human Rights held, unanimously, that there had been:

a violation of Article 8 (right to respect for private life and correspondence) of the European Convention on Human Rights.

The case concerned the system of secret interception of mobile telephone communications in Russia. The applicant, an editor-in-chief of a publishing company, complained in particular that mobile network operators in Russia were required by law to install equipment enabling law-enforcement agencies to carry out operational-search activities and that, without sufficient safeguards under Russian law, this permitted blanket interception of communications.

The Court found that Mr Zakharov was entitled to claim to be a victim of a violation of the European Convention, even though he was unable to allege that he had been the subject of a concrete measure of surveillance. Given the lack of remedies available at national level, as well as the secret nature of the surveillance measures and the fact that they affected all users of mobile telephone communications, the Court considered it justified to have examined the relevant legislation not from the point of view of a specific instance of surveillance of which Mr Zakharov had been the victim, but in the abstract. Furthermore, the Court considered that Mr Zakharov did not have to prove that he was even at risk of having his communications intercepted. Indeed, given that the domestic system did not provide an effective remedy to the person who suspected that he or she was subject to secret surveillance, the very existence of the contested legislation amounted in itself to an interference with Mr Zakharov's rights under Article 8.

The Court noted that interception of communications pursued the legitimate aims of the protection of national security and public safety, the prevention of crime and the protection of the economic well-being of the country. However, in view of the risk that a system of secret surveillance set up to protect national security might undermine or even destroy democracy under the cloak of defending it, the Court had to be satisfied that there were adequate and effective guarantees against abuse.

The Court concluded that the Russian legal provisions governing interception of communications did not provide for adequate and effective guarantees against arbitrariness and the risk of abuse which was inherent in any system of secret surveillance, and which was particularly high in a system such as in Russia where the secret services and the police had direct access, by technical means, to all mobile telephone communications.

In particular, the Court found shortcomings in the legal framework in the following areas: the circumstances in which public authorities in Russia are empowered to resort to secret surveillance measures; the duration of such measures, notably the circumstances in which they should be discontinued; the procedures for authorising interception as well as for storing and destroying the intercepted data; the supervision of the interception. Moreover, the effectiveness of the remedies available to challenge interception of communications was undermined by the fact that they were available only to persons who were able to submit proof of interception and that obtaining such

1. Grand Chamber judgments are final (Article 44 of the Convention).
All final judgments are transmitted to the Committee of Ministers of the Council of Europe for supervision of their execution. Further information about the execution process can be found here: www.coe.int/t/dghl/monitoring/execution.

proof was impossible in the absence of any notification system or possibility of access to information about interception.

Principal facts

The applicant, Roman Zakharov, is a Russian national who was born in 1977 and lives in St Petersburg. He is the editor-in-chief of a publishing company and subscribed to the services of several mobile network operators.

In December 2003 Mr Zakharov brought judicial proceedings against three mobile network operators, the Ministry of Communications, and the Department of the Federal Security Service for St Petersburg and the Leningrad Region, complaining about interference with his right to privacy of his telephone communications. He maintained that, under the relevant national law – namely, the Operational-Search Activities Act of 1995 (the OSSA), the Code of Criminal Procedure of 2001 (the CCrP) and, more specifically, Order no. 70 issued by the Ministry of Communications which requires telecommunications networks to install equipment enabling law-enforcement agencies to carry out operational-search activities – the mobile operators had permitted unrestricted interception of all telephone communications by the security services without prior judicial authorisation. He asked the district court in charge to issue an injunction to remove the equipment installed under Order no. 70, and to ensure that access to telecommunications was given to authorised persons only.

The Russian courts rejected Mr Zakharov's claim. In a judgment upheld in April 2006, the district court found, in particular, that he had failed to prove that his telephone conversations had been intercepted or that the mobile operators had transmitted protected information to unauthorised persons. Installation of the equipment to which he referred did not in itself infringe the privacy of his communications.

Complaints, procedure and composition of the Court

Relying on Article 8 (right to respect for private life and correspondence) of the European Convention, Mr Zakharov complained about the system of covert interception of mobile telephone communications in Russia. He argued in particular that the relevant national law permitted the security services to intercept, through technical means, any person's communications without obtaining prior judicial authorisation, alleging that such legislation permitted blanket interception of communications. He further relied on Article 13 (right to an effective remedy), complaining that he had no effective legal remedy at national level to challenge that legislation.

The application was lodged with the European Court of Human Rights on 20 October 2006. On 11 March 2014 the Chamber to which the case had been allocated relinquished jurisdiction in favour of the Grand Chamber[2]. A Grand Chamber hearing was held on the case on 24 September 2014.

Judgment was given by the Grand Chamber of 17 judges, composed as follows:

Dean **Spielmann** (Luxembourg), *President*,
Josep **Casadevall** (Andorra),
Guido **Raimondi** (Italy),
Ineta **Ziemele** (Latvia),
Mark **Villiger** (Liechtenstein),
Luis **López Guerra** (Spain),
Khanlar **Hajiyev** (Azerbaijan),

[2] Under Article 30 of the European Convention on Human Rights, "Where a case pending before a Chamber raises a serious question affecting the interpretation of the Convention or the Protocols thereto, or where the resolution of a question before the Chamber might have a result inconsistent with a judgment previously delivered by the Court, the Chamber may, at any time before it has rendered its judgment, relinquish jurisdiction in favour of the Grand Chamber, unless one of the parties to the case objects."

Angelika **Nußberger** (Germany),
Julia **Laffranque** (Estonia),
Linos-Alexandre **Sicilianos** (Greece),
Erik **Møse** (Norway),
André **Potocki** (France),
Paul **Lemmens** (Belgium),
Helena **Jäderblom** (Sweden),
Faris **Vehabović** (Bosnia and Herzegovina),
Ksenija **Turković** (Croatia),
Dmitry **Dedov** (Russia),

and also Lawrence **Early**, *Jurisconsult.*

Decision of the Court

Article 8 (right to private life and correspondence)

The Court found that Mr Zakharov was entitled to claim to be a victim of a violation of the European Convention, even though he was unable to allege that he had been the subject of a concrete measure of surveillance. Given the secret nature of the surveillance measures provided for by the legislation, their broad scope (affecting all users of mobile telephone communications) and the lack of effective means to challenge them at national level (see point 6 below), the Court considered that it was justified to examine the relevant legislation not from the point of view of a specific instance of surveillance, but in the abstract. Furthermore, the Court considered that Mr Zakharov did not have to prove that he was even at risk of having his communications intercepted. Indeed, given that the domestic system did not afford an effective remedy to the person who suspected that he or she was subjected to secret surveillance, the very existence of the contested legislation amounted in itself to an interference with Mr Zakharov's rights under Article 8.

It was not in dispute between the parties that interception of mobile telephone communications had had a basis in Russian law, namely the OSAA, the CCrP, the Communications Act and Orders issued by the Ministry of Communications (in particular Order no. 70), and pursued the legitimate aims of the protection of national security and public safety, the prevention of crime and the protection of the economic well-being of the country.

However, the Court concluded that the Russian legal provisions governing interception of communications did not provide for adequate and effective guarantees against arbitrariness and the risk of abuse.

In particular, the Court found shortcomings in the legal framework in the following areas:

1. **The circumstances in which public authorities are empowered to resort to secret surveillance measures**

   Notably, Russian legislation lacks clarity concerning some of the categories of people liable to have their telephones tapped, namely a person who may have information about an offence or information relevant to a criminal case or those involved in activities endangering Russia's national, military, economic or ecological security. For example, as concerns the latter category, the OSAA leaves the authorities an almost unlimited degree of discretion in determining which events or acts constitute such a threat and whether that threat is serious enough to justify secret surveillance;

2. **The duration of secret surveillance measures**

   Notably the provisions on the circumstances in which secret surveillance measures must be discontinued do not provide sufficient guarantees against arbitrary interference.

Regrettably, the requirement to discontinue interception when no longer necessary is only mentioned in the CCrP and not in the OSAA. This means in practice that interception of communications in criminal proceedings have more safeguards than interceptions in connection with activities endangering Russia's national, military, economic or ecological security;

3. **The procedures for destroying and storing intercepted data**

In particular, the domestic law permits automatic storage for six months of clearly irrelevant data in cases where the person concerned has not been charged with a criminal offence and, in cases where the person has been charged with a criminal offence, it is not sufficiently clear as to the circumstances in which the intercepted material will be stored and destroyed after the end of a trial;

4. **The procedures for authorising interception**

The authorisation procedures are not capable of ensuring that secret surveillance measures are ordered only when necessary.

Most notably, Russian courts do not verify whether there is a reasonable suspicion against the person for whom interception has been requested or examine whether the interception is necessary and justified. Thus, interception requests are often not accompanied by any supporting materials, judges never request the interception agency to submit such materials and a mere reference to the existence of information about a criminal offence or activities endangering national, military, economic or ecological security is considered to be sufficient for the interception to be authorised.

Furthermore, the OSAA does not contain any requirements concerning the content either of the request for interception or of the interception authorisation, meaning that courts sometimes grant interception authorisations which do not mention a specific person or telephone number to be tapped, but authorise interception of all telephone communications in the area where a criminal offence has allegedly been committed, and on occasions without mentioning the duration of the authorised interception. Furthermore, the non-judicial urgent procedure provided by the OSAA (under which it is possible to intercept communications without prior judicial authorisation for up to 48 hours) lacks sufficient safeguards to ensure that it is used sparingly and only in duly justified cases.

Moreover, a system, such as the Russian one, which allows the secret services and the police to intercept directly the communications of each and every citizen without having to show an interception authorisation to the communications service provider, or to anyone else, is particularly prone to abuse. This system results in particular in the secret services and the police having the technical means to circumvent the authorisation procedure and intercept communications without obtaining prior judicial authorisation. The need for safeguards against arbitrariness and abuse appears therefore to be particularly great in this area;

5. **The supervision of interception**

As it is currently organised, supervision of interception does not comply with the requirements under the European Convention that supervisory bodies be independent, open to public scrutiny and vested with sufficient powers and competence to exercise effective and continuous control. Firstly, it is impossible for the supervising authority in Russia to discover interception carried out without proper judicial authorisation as Order no. 70 prohibits the logging or recording of such interception. Secondly, supervision of interception carried out on the basis of proper judicial authorisations is entrusted to the President, Parliament and the Government, who are given no indication under Russian law as to how they may supervise interception, as well as the competent prosecutors, whose

manner of appointment and blending of functions, with the same prosecutor's office giving approval to requests for interceptions and then supervising their implementation, may raise doubts as to their independence. Thirdly, the prosecutors' powers and competences are limited: notably, information about the security services' undercover agents and their tactics, methods and means remain outside their scope of supervision. Fourthly, supervision by prosecutors is not open to public scrutiny: their semi-annual reports on operational-search measures are not published or otherwise accessible to the public. Lastly, the effectiveness of supervision by prosecutors in practice is open to doubt, Mr Zakharov having submitted documents illustrating prosecutors' inability to obtain access to classified materials on interception and the Government not having submitted any inspection reports or decisions by prosecutors ordering the taking of measures to stop or remedy a detected breach in law;

6. **Notification of interception of communications and remedies available**

Any effectiveness of the remedies available to challenge interception of communications is undermined by the fact that they are available only to persons who are able to submit proof of interception. Given that a person whose communications have been intercepted in Russia is not notified at any point and does not have an adequate possibility to request and obtain information about interceptions, unless that information becomes known to him as a result of its use in evidence in eventual criminal proceedings, that burden of proof is virtually impossible to satisfy.

The Court noted that those shortcomings in the legal framework appear to have had an impact on the actual operation of the system of secret surveillance which exists in Russia. The Court was not convinced by the Government's argument that all interceptions in Russia were performed lawfully on the basis of a proper judicial authorisation. The examples submitted by Mr Zakharov in the domestic proceedings[3] and in the proceedings before the European Court of Human Rights[4] indicated the existence of arbitrary and abusive surveillance practices, which were apparently due to the inadequate safeguards provided by law.

In view of those shortcomings, the Court found that Russian law did not meet the "quality of law" requirement and was incapable of keeping the interception of communications to what was "necessary in a democratic society". There had accordingly been a violation of Article 8 of the Convention.

Other articles

Given the findings under Article 8, in particular with regard to the notification of interception of communications and available remedies, the Court held that it was not necessary to examine Mr Zakharov's complaint under Article 13 separately.

Article 41 (just satisfaction)

The Court held, by 16 votes to one, that the finding of a violation constituted in itself sufficient just satisfaction for any non-pecuniary damage sustained by Mr Zakharov. It further held that Russia was to pay Mr Zakharov 40,000 euros (EUR) in respect of costs and expenses.

[3] In the domestic proceedings Mr Zakharov referred in particular to two judicial orders, which retrospectively authorised the interception of a number of people's telephone communications, and which, in his opinion, went to prove that the mobile network operators and law-enforcement agencies routinely resorted to unauthorised interception.

[4] In order to prove that law-enforcement officials unlawfully intercepted telephone communications without prior judicial authorisation and disclosed the records, Mr Zakharov submitted to the European Court printouts from the Internet of the transcripts of politicians' private telephone conversations and news articles reporting on the fact that anyone could buy the transcript of a private telephone conversation from the police.

Separate opinions

Judge Ziemele expressed a dissenting opinion and Judge Dedov expressed a concurring opinion which are annexed to the judgment.

The judgment is available in English and French.

Press contacts
echrpress@echr.coe.int | tel.: +33 3 90 21 42 08

Tracey Turner-Tretz (tel: + 33 3 88 41 35 30)
Nina Salomon (tel: + 33 3 90 21 49 79)
Denis Lambert (tel: + 33 3 90 21 41 09)
Inci Ertekin (tel: + 33 3 90 21 55 30)

ADVANCE UNEDITED VERSION

Distr.: General
8 March 2016

Original: English

Human Rights Council
Thirty-first session
Agenda item 3
Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development

Report of the Special Rapporteur on the right to privacy, Joseph A. Cannataci·

Note by the Secretariat

In the present report, submitted to the Human Rights Council pursuant to Council resolution 28/16, the Special Rapporteur on the right to privacy describes his vision for the mandate, his working methods and provides an insight into the state of privacy at the beginning of 2016 and a work plan for the first three years of the mandate

…

The UK's Investigatory Powers Bill

1. Recognition is due to the three joint UK Parliamentary committees: the science and technology committee on February 1, the intelligence and security committee on February 9 and most importantly, the joint committee for the bill itself on February 11, 2016 for their consistent, strong, if occasionally over-polite, criticism of the UK Government's Investigatory Powers Bill. The joint committee for the draft investigatory powers bill made 86 recommendations for changes to the bill in its report, concentrating on issues of clarity, judicial oversight and justification of the various powers. Recognition is also due to the UK Government which has taken heed of advice from various quarters and which is using the IPB to introduce much-needed reinforcement of oversight mechanisms. While there may still be some room for improvement in this area too, these are steps in the right direction. At the time of the submission of this SRP report to the HRC, the SRP's initial assessment of the latest version of the Bill published on 1 March 2016 however leads to serious concern about the value of some of the revisions most recently introduced. At the time of writing, not only do some of the UK Government's proposals appear to run counter to the logic and findings of UN Special Rapporteur on Counter-terrorism Ben Emmerson in his 2014 report dealing inter alia with mass surveillance[1], but they *prima facie* fail the benchmarks set by

· Late submission

[1] http://s3.documentcloud.org/documents/1312939/un-report-on-human-rights-and-terrorism.pdf

the ECJ in *Schrems* and the ECHR in *Zakharov*. The SRP firmly encourages the three committees of the UK Parliament commended above to continue, with renewed vigour and determination, to exert their influence in order that disproportionate, privacy-intrusive measures such as bulk surveillance and bulk hacking as contemplated in the Investigatory Powers Bill be outlawed rather than legitimised. It would appear that the serious and possibly unintended consequences of legitimising bulk interception and bulk hacking are not being fully appreciated by the UK Government. Bearing in mind the huge influence that UK legislation still has in over 25% of the UN's members states that still form part of the Commonwealth, as well as its proud tradition as a democracy which was one of the founders of leading regional human rights bodies such as the Council of Europe, the SRP encourages the UK Government to take this golden opportunity to set a good example and step back from taking disproportionate measures which may have negative ramifications far beyond the shores of the United Kingdom. More specifically, the SRP invites the UK Government to show greater commitment to protecting the fundamental right to privacy of its own citizens and those of others and also to desist from setting a bad example to other states by continuing to propose measures, especially bulk interception and bulk hacking, which *prima facie* fail the standards of several UK Parliamentary Committees, run counter to the most recent judgements of the European Court of Justice and the European Court of Human Rights, and undermine the spirit of the very right to privacy. Finally, the SRP invites the UK Government to work closely with the mandate, especially in the context of its thematic study on surveillance, in an effort to identify proportionate measures which enhance security without being overly privacy-intrusive.