Can Courts Provide Effective Remedies Against Violations of Fundamental Rights by Mass Surveillance? The Case of the United Kingdom

Felix Bieker

Can Courts Provide Effective Remedies against Violations of Fundamental Rights by Mass Surveillance? The Case of the United Kingdom

Felix Bieker

Walther Schücking Institute for International Law at the University of Kiel and ULD (Independent Centre for Privacy and Data Protection) Schleswig-Holstein, Kiel, Germany
fbieker@datenschutzzentrum.de

Abstract: This case comment examines the Investigatory Powers Tribunal's jurisdiction and critically analyses its recent finding of compatibility of the GCHQ's mass surveillance of telecommunications in the case of Liberty v. GCHQ with human rights. The analysis shows that the Tribunal's human rights assessment fails to meet ECtHR standards. It provides a brief outlook on the cases concerning UK mass surveillance pending before the ECtHR and the reform of the RIPA regime, which expands the GCHQ's competences even further. It concludes that neither the Tribunal's jurisprudence nor the current reform process alleviate concerns regarding the mass surveillance's compatibility with human rights.

Keywords: Investigatory Powers Tribunal, GCHQ, NSA, RIPA, Draft Investigatory Powers Bill, Mass Surveillance, Privacy, Snowden Documents, European Convention on Human Rights, Tempora, Prism.

> *Indeed, it would defy the purpose of government efforts to keep terrorism at bay, thus restoring citizens' trust in their abilities to maintain public security, if the terrorist threat were paradoxically substituted for by a perceived threat of unfettered executive power intruding into citizens' private spheres by virtue of uncontrolled yet far-reaching surveillance techniques and prerogatives* – ECtHR, Szabo and Vissy v. Hungary, App. no. 37138/14, Judgment of 12 January 2016, para. 68.

1 Introduction

The documents leaked by Edward Snowden in 2013 informed the general public about the practices of the US National Security Agency (NSA) and its UK counterpart, the Government Communications Headquarters (GCHQ) to tap into electronic communications on a massive scale. This case comment, as the judgments analysed, will focus on the major programs: With its Upstream program the NSA accesses in-

formation from fibre-optic cables, while under its Prism program it obtained access to the networks of technology companies such as Google, Microsoft, Facebook and Apple for in-depth surveillance of online communication [1]. This information is shared with GCHQ [2], which in turn shares information it gathers in its own mass surveillance program: Tempora enables GCHQ to access the fibre-optic cables transporting internet traffic and phone calls, which cross the British isles [3].

In the meantime, further details about surveillance programmes of both the NSA and GCHQ, as well as similar programmes of inter alia the French intelligence services, have become public [4]. Additionally, cooperation between NSA and other European intelligence services, such as the German BND, has been in the focus [5, 6].

However, as only Tempora and Prism/Upstream have been subject to judicial scrutiny, the present article will address these programmes. The UK Investigatory Powers Tribunal (IPT or the Tribunal) as well as the European Court of Human Rights (ECtHR) were asked to rule on the compatibility of these programmes with the European Convention on Human Rights (ECHR), namely the right to privacy as guaranteed by Article 8 ECHR [7, 8, 9, 10, 11, 12].

In line with this Summer School's topical question concerning the need for a revolution, this case comment analyses the judicial response to the Snowden revelations. As a substantial amount of time has passed since the first revelations on the activities of GCHQ, the question is whether the existing legal framework is apt to provide sufficient remedies for these actions or whether they require a revolutionary reform. In the following, this article will set out the UK legal framework for the exchange of information with other intelligence services and the operation of interception of communications by GCHQ (2), detail the requirements of the ECHR with regard to measures of secret surveillance (3) and focus on the proceedings before the IPT (4). It will then critically evaluate the Tribunal's findings (5) and in an outlook turn to the proceedings instigated before the ECtHR, to provide guidance on possible outcomes and outline efforts to reform the regime of surveillance as well as judicial oversight (6), before drawing final conclusions (7) on this matter.

2 The UK Legal Framework

2.1 The Mission of the Intelligence Services

According to Section 3 of the Intelligence Services Act (ISA), GCHQ is competent to monitor electronic signals and gather information relating to national security, the economic well-being of the United Kingdom and to support the prevention and detection of serious crime. Under Section 4(2) ISA it is for the Director of GCHQ to ensure that information is obtained only in as far as it is necessary for the proper achievement of its functions. Similar clauses are contained in the relevant provisions for the Security Service, also known as MI5, and the Secret Intelligence Service, better known as MI6. All information obtained by an intelligence service may be used in relation to any of its functions, as emphasized by Section 19(2) Counter-Terrorism Act.

2.2 Measures of Secret Surveillance

Measures of secret surveillance and their review are laid down in the Regulation of Investigatory Powers Act (RIPA). Section 1 RIPA contains a general prohibition of any interception of communications, unless there is an interception warrant as prescribed by Section 5 RIPA. In order to obtain such a warrant GCHQ must apply to the Secretary of State under Section 6 RIPA, who may order the interception and disclosure of communications during their transmission in the interests of national security, the economic well-being of the United Kingdom or the prevention and detection of serious crime. According to Section 5(2) RIPA the Secretary of State has to believe that the warrant is necessary and proportionate to achieve one of these goals.

Interception warrants based on national security or the economic well-being are valid for six months, those relating to the detection and prevention of serious crime for three. Both kinds may be repeatedly extended for another six or three months, respectively, according to Section 9(1) and (6) RIPA, if the Secretary of State believes that this continues to be necessary for the reasons set out under Section 5(3) RIPA.

Section 8 RIPA then distinguishes between targeted and strategic warrants: targeted warrants under Section 8(1) RIPA are directed against specific individuals or premises. Strategic warrants according to Section 8(4) and (5) RIPA concern the interception of external communications, which is of interest here. This term is defined in Section 20 RIPA as any communication, which is either sent or received outside the United Kingdom. As, on a technical level, such a differentiation is not possible, the interception entails a two-step process: firstly, all communications are intercepted. In a second step, intercepted material may only be processed where it has been verified that its examination is necessary for the reasons of Section 5(3)(a-c) RIPA and it is believed that the person concerned is not within the United Kingdom, as prescribed by Section 16 RIPA

As a safeguard, Section 15 RIPA demands that any information obtained under Section 8 RIPA must be made accessible or distributed only as much as necessary and be destroyed once this is no longer the case. Under Section 15(4)(a) RIPA necessity means that it is likely that the information is needed for the any of the purposes of Section 5(3) RIPA, i.e. national security, the economic well-being or the detection and prevention of serious crime.

3 Requirements of the ECHR

As any national legislation, the RIPA regime has to adhere to the human rights requirements of the ECHR, as implemented by the Human Rights Act. It is not the task of the ECtHR to review national legislation in abstracto, but rather to assess whether the application of a law gives rise to a violation of the Convention. This is due to the fact, that the ECtHR is competent to interpret the ECHR under Art. 32(1) ECHR, while it is the task of national courts to interpret national legislation. Thus, in order to lodge an individual complaint under Art. 34 ECR, the applicant has to submit that he or she is directly affected by the measure concerned. However, when it comes to measures of secret surveillance, this requirement has to be adjusted, as – due to the

very nature of the measure – the individual concerned is unaware whether he or she is affected. Consequently, an applicant can possibly be affected by a measure either because he or she belongs to a group of persons targeted by the legislation or because the provisions directly affect all users of a communication service as the communications are intercepted in bulk [13, para. 171]. In a second step, the standard of review by the ECtHR depends on the availability of remedies to persons suspecting to be subjects of secret surveillance: if such remedies are not available, the sole menace of surveillance is a direct interference with the rights of the ECHR. In contrast, if there are effective remedies available, the applicant must demonstrate that due to his or her personal situation he or she is potentially at risk.

Article 8 ECHR is the relevant provision for the questions at hand in this case, as it protects the private life of a person. The provision itself contains various individual rights, which are all related to the notion of private life.

Most relevant here is the right to privacy, as enshrined in Article 8(1) ECHR: the right to privacy awards protection from measures of surveillance even beyond a person's home [14, para. 27]. This includes individual communications, whereby e.g. communications by telephone are protected as correspondence as well as under aspects of privacy [14, para. 28]. An interference with the right to privacy occurs, where measures to obtain information are used by the State, inter alia measures of secret surveillance [15, para. 41]. With regard to the protection of personal correspondence it is not necessary that contents are accessed – even where only metadata, i.e. data concerning the subscriber, the receiver, the time and duration of a communication, are made accessible to public authorities there is an interference [16, paras. 83 et seq.].

Article 8(1) ECHR further includes the right to the protection of personal data as a subcategory of the right to privacy [17, § 22 para. 10]. Each collection, storage or processing of such data constitutes a separate interference with this right [18, para. 48].

Like most rights of the ECHR, Article 8 it is not an absolute right, but may be restricted in accordance with the justifications clause of Article 8(2) ECHR. It may inter alia be restricted with regard to national security, the economic well-being of the State and for the prevention of serious crime, if the restriction is accordance with the law and necessary in a democratic society. The ECtHR has introduced specific requirements concerning the quality of a law in order to justify interferences under Article 8(2) ECHR: while the provisions do not necessarily have to be statutory law, they have to be sufficiently accessible and foreseeable [18, para. 67; 19, para. 76]. Particularly with regard to measures of secret surveillance there can be no unfettered discretion of public authorities; there must be limitations in order to allow for the review of such acts [19, para. 78]. Further, there have to be sufficient signposts to enable individuals to foresee on an abstract level, when they may become subjects of surveillance measures in order to prevent arbitrariness in the exercise of these powers [15, paras. 42 and 49]. While this must not be read as an obligation to inform an individual of specific surveillance measures – which, of course, would be detrimental to their very purpose – there have to be sufficient and effective safeguards against abuse [16, para. 67]. Measures striving to protect national security must not undermine or even destroy democracy [15, paras. 49 et seq.].

Accordingly, there can be no indiscriminate collection of data without provisions limiting the powers of a secret police [20, paras. 57 et seq.]. In its seminal *Weber* decision, the ECtHR set out specific requirements for telephone-tapping: the law has to define the offences which may trigger surveillance measures as well as the persons potentially affected by such measures [21, para. 95]. Further, limitations as to the duration of the measures and the procedure of processing the data have to be laid out. Lastly, there have to be safeguards with regard to the sharing of the data and their proper destruction.

Regarding a measure's necessity in a democratic society, the ECtHR generally awards the Contracting Parties a wide margin of appreciation when it comes to measures concerning national security [18, para. 59]. As the ECHR is an international treaty between 47 European States, it is intended to provide a minimum standard for the protection of fundamental rights. In order to accommodate the different political systems and to respect the national sovereignty of the Contracting Parties, the ECtHR allows them a certain amount of discretion in justifying national measures which interfere with fundamental rights. This discretion varies, depending on the measure and the area of concern. However, the ECtHR has embraced the approach of the European Court of Justice to apply a test of strict necessity in the assessment of secret surveillance measures, due to their great potential for abuse [22, para. 73].

As a last step, the assessment of proportionality calls for the striking of a balance between the interest of national security and the effect of secret surveillance measures on an individual [21, para. 106]. Thus, the result also depends on the gravity of the interference with the individual's rights [14, para. 98].

4 Oversight by the Investigatory Powers Tribunal

4.1 The Functions of the Investigatory Powers Tribunal

The judicial supervision of surveillance measures rests with the Investigatory Powers Tribunal as a specialized court for the intelligence services established under Section 65 RIPA. According to Section 65(2)(a) RIPA this includes applications for judicial review concerning individual rights of the ECHR under Section 7(1)(a) HRA, when they concern actions of the intelligence services. At the end of the proceedings, the IPT makes a Determination as to whether it upholds the claims brought before it according to Section 68(4) RIPA.

4.2 The Judgments Against GCHQ

Soon after the Snowden revelations, British advocacy groups Liberty, Privacy International and Amnesty International applied for judicial review before the IPT. They claimed violations of their right to privacy under Article 8 ECHR and their right to freedom of speech according to Article 10 ECHR [7, paras. 5, 14 and 79]. The claimants saw no appropriate provisions for the exchange of information with the

NSA and found the legal requirements for the interception of information transmitted by fibre-optic cables insufficient. The Tribunal, however, decided that Article 10 ECHR did not entail any questions beyond those posed by Article 8 ECHR and thus restricted its review to the right to privacy [7, para. 12].

4.3 The Judgment of 5 December 2014

In its judgment of 5 December 2014, the Tribunal addressed two substantive points raised by the claimants.

4.3.1 The Exchange of Information (Prism/Upstream)

Concerning the first part of the action, the Tribunal assumed that the NSA collected communications from US service providers and that among those were such of the claimants, which was then forwarded to the British intelligence services [7, para. 14]. This raised the question, whether the legal regime was in accordance with the law as prescribed by Article 8(2) ECHR.

The intelligence services and the government as respondents argued that the competence to exchange information with other intelligence services followed from the general functions of the intelligence services as detailed above (2.1), which included appropriate limitations [7, paras. 19 et seq.]. They had access only with regard to their functions, which corresponded to those of interception warrants under Section 8 RIPA. The respondents strove to show that while there was an interference with the right of privacy of individuals concerned by this practice, it was a much lighter interference as it would be in cases where the GCHQ itself intercepted communications [7, paras. 34-36].

The Tribunal first examined whether the legal regime was in accordance with the law. It therefore referred to the ECtHR's judgments in *Malone* and *Bykov* when stating that for an interference to be in accordance with the law, public authorities were not to be given unfettered discretion and there needed to be appropriate safeguards against abuse [7, para. 37]. Further, the provisions needed to be sufficiently clear and foreseeable. The IPT held that the rules did not have to be implemented as statutory law, when there was sufficient signposting and effective supervisory mechanisms [7, paras. 38 et seq.]. While the arrangements further specifying the general provisions where confidential, they were monitored by the parliamentary Intelligence and Security Committee and the Interception of Communications Commissioner, who ensured that the intelligence services acted in compliance with these rules [7, paras. 42-44 and 22-24]. Further, judicial oversight was provided by the IPT itself with its extensive powers of investigation under Section 68(6) RIPA [7, para. 47]. In the course of a confidential hearing, the intelligence services disclosed that requests for information were made to foreign intelligence services only under an international mutual legal assistance agreement or in analogy to the rules on interception warrants under Section 8(1) or (4) RIPA. In cases where there was no interception warrant, communications could only be requested exceptionally, if RIPA was not thereby circumvented and it was necessary and proportionate for the intelligence services to receive the information. These latter requests could be issued only by the Secretary of State and had so

far never occurred in practice [7, paras. 47 and 51]. In any case, all information thus obtained was treated in accordance with the safeguard clauses of Sections 15 and 16 RIPA.

Thus, the IPT concluded that there were appropriate provisions to ensure that the exchange of information was in accordance with national law as well as Articles 8 and 10 ECHR and that after the disclosures made by the respondents, these rules were sufficiently accessible [7, para. 55]. It was also satisfied with the level of supervision and found that the limitations on the discretion of the security services were adequate to prevent arbitrary interferences.

4.3.2 The interception of external communications (Tempora)

For examining the compatibility of the interception of external communications with Article 8 ECHR, the Tribunal assumed that the claimants' communications could have been intercepted and parts thereof might have been processed [7, para. 59]. The claimants argued that GCHQ with its Tempora programme intercepted all communication contents and their metadata which were transmitted by fibre-optic cables [7, para. 78]. These were then stored for an undefined period of time and searched automatically with selectors provided inter alia by the NSA and eventually forwarded to other public authorities.

It thus had to be assessed whether the difficulty in differentiating between internal and external communications led to an incompatibility of Section 8(4) RIPA with the requirements of Article 8(2) ECHR. As even communications only sent within the UK could entirely or partly be transmitted via cables outside the UK, this did not make them external communications [7, paras. 93 et seq. and 68 et seq.]. However, this was the reason why Section 8(5)(b) in conjunction with Section 5(6) RIPA allowed the interception of internal communications as a collateral. Yet, the Tribunal found that these collaterally intercepted communications were concerned only at a preliminary stage and subsequently treated differently for the purposes of Section 16 RIPA [7, paras. 101 et seq.]. As under this provision, material intercepted under Section 8(4) RIPA may only be accessed where it is assumed that the person concerned is not within the UK, it was ensured that internal communications were not used. However, Section 16 RIPA only concerns intercepted material, which under the definition of Section 20 RIPA includes only contents of communications, whereas related communications data, which are also defined by Section 20 RIPA, are not covered [7, paras. 107-109]. Related communications data can also be described as metadata. The respondents argued that the collection of metadata was a much lighter interference with the right to privacy than the collection of contents of communications. In order to underline this argument, the respondents referred to the judgment of the Court of Justice of the European Union (CJEU) in the *Digital Rights Ireland* case.[1] In this case, the CJEU invalidated the EU Data Retention Directive 2006/24/EC on the

[1] For an in-depth assessment of the judgment cf. Bieker, F.: The Court of Justice of the European Union, Data Retention and the Rights to Data Protection and Privacy – Where are we now?. In: Camenisch, J. et al. (eds.) Privacy and Identity 2014. IFIP AICT 457, pp. 73-86. Springer, Heidelberg (2015).

grounds that the bulk collection of online and telephone communications metadata was incompatible with the rights to privacy and data protection under the EU's fundamental rights. The respondents in the case at hand argued that the CJEU did so only due to the directive's missing nexus to a threat to the public order and missing limitations on the access of national authorities [23, paras. 59 et seq.]. Unlike the EU directive the national legislation of the UK, more precisely Section 8(4) RIPA on strategic warrants, was explicitly linked with a threat to national security or serious crime according to Section 5(3) RIPA. Furthermore, the metadata were required to make the determination under Section 16 RIPA whether the person concerned was within the UK [7, para. 112]. The IPT concurred, stating the limiting of the access to metadata for this purposes appeared as a "impossibly complicated or convoluted course" [7, para. 113]. The collection of metadata could also be justified under Section 15(3) and (4) RIPA for later use by the intelligence services for the reasons set out in Section 5(3) RIPA. As these data were not to be stored longer than necessary, the IPT held that the ECtHR's requirements concerning the minimum safeguards for surveillance measures were also satisfied [7, paras. 112 and 114].

When assessing the rules of RIPA as a whole, the Tribunal recapitulated the ECtHR's requirements as set out in the *Weber* case. Firstly, it thus examined whether the nature of the offences which could trigger an interception warrant and the persons potentially affected, were sufficiently clear to prevent abuse. Concerning the aim of national security, it cited the case of *Kennedy*, where the ECtHR determined that the notion of national security was sufficiently clear and explicitly mentioned in Article 8(2) ECHR [7, para. 116 i)]. While it was not possible to distinguish between groups of persons with regard to internal or external communications on the first level of interception, the IPT found this to be inevitable [7, para. 116 ii)]. There was also no need for a predefined list of search terms to determine which communications would be further examined, as this would hinder the execution of the warrants and was unrealistic [7, para. 116 v)]. As the ECtHR had already ruled that there were sufficient safeguards with regard to the supervision by the Interception of Communications Commissioner and the extensive jurisdiction of the IPT itself, the Tribunal was satisfied that for strategic warrants, just as for targeted warrants, there was no need for a judicial pre-authorization [7, para. 116 vi)].

Secondly, the IPT examined the requirements regarding the duration of the surveillance measures and the procedure concerning the examination, use and storage as well as destruction of the intercepted information [7, para. 117]. These are laid down in Section 15 RIPA, the Code and the arrangements, which satisfied the requirements concerning the quality of the law as not all the details of the procedure needed to be statutory law.

Lastly, the Tribunal came to the question of proportionality, stating that a balance between the interest of national security and the gravity of the interference had to be achieved [7, para. 119]. Highlighting again the Interception of Communications Commissioner and its own jurisdiction, it held that there were adequate and effective measures in place to prevent the abuse of power. Additionally, the rules on the procedure for the issuance of warrants were sufficiently clear to ensure their foreseeability [7, paras. 120 et seq.]. As the ECtHR had already held in *Kennedy* with regard to the

interception of internal communications, the safeguards of Section 15 RIPA satisfied the *Weber* requirements as they clearly laid down the duration of and possibilities to extend surveillance measures [7, para. 123]. Even though these could be extended indefinitely, the Secretary of State had to ensure each time that interception was still necessary. Section 15 RIPA also included appropriate safeguards concerning data security, while the Code further defined the persons competent to access the information and ensured that they were destroyed, if no longer necessary. Thus, the Tribunal concluded that with regard to the Tempora programme there was also no violation of Articles 8 and 10 ECHR.

4.4 The Judgment of 6 February 2015

Following up on its pronouncement that, with the disclosures made by the respondents during the initial hearings, the requirements of Article 8(2) ECHR were fulfilled, the Tribunal examined the period before these disclosures in a separate judgment. It found that without the explanations regarding the handling of requests to foreign intelligence services in analogy to Section 8(1) and (4) RIPA, there were no sufficient signposts as to the implementation of this practice [8, paras. 14-21]. Therefore, these provisions were not sufficiently accessible and foreseeable and thus did not meet the requirements of Article 8(2) ECHR. Thus, the exchange of information with foreign intelligence services prior to the disclosures violated Articles 8 and 10 ECHR. Although in this case, the IPT ruled against the government and the GCHQ, both judgments were subject to wide-spread criticism, which will be addressed in the following section.

5 Assessment of the Proceedings Before the Investigatory Powers Tribunal

In the introduction to its judgment of 5 December 2014 the Tribunal sets the scene for the assessment of possible violations of fundamental rights when it states that the relevant actions of the intelligence services are to be regarded in the context of national security [7, para. 6]. It stresses that international terrorism threatens the United Kingdom specifically and that further attacks are very likely to occur.

The provisions of RIPA as a whole are phrased in a very broad manner, which is manifested already in Section 5(2) RIPA, which allows the interception of communications for the far-reaching goals of national security, the economic well-being of the UK and the detection and prevention of serious crime. In order to issue such an interception, the Secretary of State only has to assume, that such a measure will serve one of these aims and is proportionate. With this subjectively phrased criterion, it is questionable, whether the issuance of an interception warrant can even be subject to any form of independent review [24, p. 652]. This gives the Secretary of State considerable discretion in how to interpret the evidence. If instead the provision required that the measure had to objectively serve one of the aims and be proportionate, the discre-

tion of the Secretary of State would be limited and would allow for an independent assessment by a court.

Additionally, as shown above, the issuance of strategic warrants under Section 8(4) RIPA allows for collection of vast amounts of data. It does not only cover the interception of all communications where one of the subscribers is outside the UK, but also includes a comprehensive collection of metadata of any communications. This includes both internal and external communications, as the safeguards clause of Section 16 RIPA, which makes a further examination of information subject to further requirements, applies only to the contents of communications according to Section 20 RIPA. This leaves a loophole for the unfettered interception of metadata, which may be stored if it is likely that it may become useful with regard to the legitimate – and rather broad – aims of Section 5(3) RIPA. While the IPT is right when it states that the collection and use of metadata is a lighter interference than the collection and use of the contents of communications, it has to be stressed that even metadata allow very detailed insights into the life of a person. This contention was shared by the CJEU in its judgment in the case of *Digital Rights Ireland* [23, paras. 47, 54 et seq.]. It found the data retention envisaged by the directive likely to create a feeling of constant surveillance in all citizens due to its massive scale. While the respondents before the IPT contended that the CJEU only invalidated the directive because of a missing link to a threat to public security and insufficient restrictions on access of national authorities, there is more to the judgment than they let on. The requirements established by the CJEU with regard to the handling of the data and data security are indeed derived from the ECtHR's jurisprudence. Yet, the CJEU emphasized the need for the protection of individual communications due to the mass-scale and the particularly grave interference with the right to private life and data protection. It therefore opted for a strict review of the proportionality of the measure.

After the directive had been invalidated, member States were called upon to adapt their national implementation measures. While some national courts, inter alia in Austria, Slovakia, Slovenia and Romania, annulled the national legislation, other member States opted for reform [25, 26]. Amongst the latter group was the UK, where the government chose to fast-track legislation on data retention in a controversial manner [27]. Parliament enacted a new bill on data retention, the Data Retention and Investigatory Powers Act (DRIPA). The bill also included changes to RIPA: under Section 4 DRIPA the legal regime of RIPA is extended extraterritorially, to enable the UK to issue interception warrants to foreign communications service providers which offer their services in the UK [28]. However, after two Members of Parliament applied for judicial review of the act, the High Court in July 2015 ruled that the provisions regarding access to and use of the data were not sufficiently clear and objected to the fact that retention notices were not subjected to judicial or any other independent preauthorization [29, para. 114]. Thus, the High Court decided that Section 1 DRIPA had to be disapplied after 31 March 2016. However, the judgment deals only with data retention and not with the extension of RIPA and is currently under review in an appeal to the Supreme Court, which referred the case to the CJEU under the preliminary reference procedure of Art. 267 TFEU. There, the case has been fast-tracked and will thus swiftly provide an answer to the questions referred on the measure's compatibil-

ity with EU fundamental rights and the CJEU's own judgment in *Digital Rights Ireland* [30].

Both the judgments of the CJEU and the High Court highlight the considerable issues the collection of metadata entails. With its judgment, the High Court has set limits, which have to be applied to similar contexts, such as the even more invasive collection of the contents of communications. This is even more so as the IPT did not even require the advance definition of search terms with regard to the interception of external communications under Section 8(4) RIPA.

The way the Tribunal compares the interception of internal communications under Section 8(1) RIPA and that of external communications under Section 8(4) RIPA is also troubling. In this context, the IPT cites the ECtHR's judgment in *Kennedy* to justify that strategic warrants do not require judicial pre-authorisation. Similarly, it argues with regard to the safeguards of Section 15 RIPA, which in its own reasoning make the surveillance measures lawful, even though they can be extended indefinitely. When it refers to *Kennedy*, the IPT refuses to admit the striking differences between the interception of internal and external communications. While individual warrants are directed against a specifically defined person or premise, this is not the case for strategic warrants [24, p. 652 et seq.]. They are indiscriminate measures with a much broader scope and therefore require more safeguards than the more specific and limited individual warrants.

Furthermore, the Tribunal's assessment of proportionality does not meet the requirements of the ECtHR, which it nonetheless cites. Instead of striking a balance between national security and the individual rights, the IPT is focused solely on the requirements of national security. It merely refers to the safeguards against abuse, i.e. the Interception of Communications Commissioner, its own jurisdiction and Section 15 RIPA, but in no instance does it actually assess the gravity of the interference with the right to privacy.

Concerning the exchange of information with the NSA, the IPT argued that the interference with the claimants' rights was less severe than if the GCHQ itself intercepted the information. Unfortunately, it did not further elaborate this contention, which seems questionable. From a fundamental rights perspective it does not make a difference for the individual whether his or her information is obtained by GCHQ or the NSA, if it ends up in the databases of the GCHQ either way. If anything, this argument sounds as though it was trying to allow GCHQ to escape its fundamental rights obligations by using the NSA for the collection of information.

Yet, the Tribunal's arguments concerning the lawfulness of the exchange of information in analogy to Section 8(4) RIPA is even more troubling. As has been shown, these provisions are also subject to grave concerns regarding their proportionality. While it is fortunate, that the Tribunal at least found the intelligence services' practice to be unlawful until the disclosures of the respondents, the proceedings were not transparent for the public, with the closed hearings of the respondents and even the latter judgment in no way affected their operation of the surveillance measures [31, 32, 33].

6 Outlook

6.1 The Proceedings Pending Before the European Court for Human Rights

Shortly after the Snowden revelations, in September 2013, several British advocacy groups and the spokesperson of German advocacy group Chaos Computer Club applied to the ECtHR with an individual complaint based on a violation of Article 8 ECHR [11]. They submit that there is no legal basis for the exchange of information with the NSA and that the legal regime governing strategic warrants is insufficient as it entails mass-scale interception of communications. These warrants are then continuously extended and the notion of national security is too vague. Lastly, the groups allege that the indiscriminate interception of external communications is disproportionate.

In September 2014 another application was filed by the Bureau of Investigative Journalism (BIJ) and one of their reporters, which is based on a violation of Articles 8 and 10 ECHR [12]. The BIJ is a non-profit organisation of journalists, whose high-level investigations have had an international impact. Except for the exchange of information with the NSA, it is of a similar scope to the previous application. However, it focuses on the collection of metadata and external communications.

Aside from substantive questions to the parties, the ECtHR in both proceedings included a question on the exhaustion of domestic remedies [11, para. 10; 12, para. 4]. In order to lodge an application with the ECtHR all domestic remedies have to be exhausted according to Article 35(1) ECHR. Even though neither of the applicants had instigated proceedings before the IPT, the ECtHR is usually generous when it comes to this requirement and takes into account peculiarities of the respective national legal system [17, § 13 para. 23]. Further, the ECtHR points to its own case-law where it has repeatedly held that declarations of incompatibility under Section 4 HRA are not an adequate judicial remedy, as they oblige neither the executive nor the legislature to change the national law [34, paras. 40-44].

After the IPT's judgments, the applicants in these proceedings also lodged a complaint with the ECtHR [35]. The advocacy groups argue that the rules on the exchange of foreign communications under Prism and Upstream are excessively broad and that the Tempora programme does not comply with the minimum statutory requirements set out by the ECtHR. Besides these complaints under Articles 8 and 10 ECHR, they further contend that the IPT wrongly held closed hearings and thus violated the right to a fair hearing under Article 6 ECHR and that the framework for the interception of foreign communications under Section 8(4) RIPA is discriminatory on grounds of nationality and national origin and thus in violation of Article 14 taken in conjunction with Articles 8 and 10 ECHR.

While it is hardly possible to predict the outcome of these proceedings, especially as considerations of proportionality will be paramount, a few points for debate can be identified. The ECtHR, in previous decisions, has repeatedly referred to and taken inspiration from the rights of the European Charter of Fundamental Rights as interpreted by the CJEU, most recently in a case concerning the right to privacy [36, paras. 55 et seq.]. It is not inconceivable that the ECtHR in the cases at hand may draw on

the ruling of the CJEU. On the other hand there may be considerable pressure on the ECtHR by the British government, which is generally sceptical of the court's rulings [37]. The Conservative Party even detailed plans to leave the ECHR system [38].[2]

While the strictness of the ECtHR in its proportionality review depends on the legitimate aim it usually awards more discretion when it comes to measures in the interest of national security. However, RIPA relies on the prevention and detection of serious crime as well as the economic well-being. While the latter has now been put in the context of national security by amendments made to Section 5(3) RIPA by Section 3 DRIPA, the ECtHR awards less room for manoeuvre when it comes to reasons other than national security [14, para. 98]. Furthermore, the ECtHR has in the context of searches increased its scrutiny of the national provisions when there was no judicial pre-authorisation for these measures [39, para. 45]. In any case, with the judgments of the IPT the ECtHR has much to review.

6.2 Reform of the RIPA Regime

In the wake of the Snowden revelations there have been several reports evaluating the legal regime on security services: the Intelligence and Security Committee of Parliament conducted its own review. Further, DRIPA foresaw a review of the effectiveness of current legislation and investigating whether there was a need for new or amended legislation, which was conducted by an independent expert, David Anderson QC. Additionally, an independent report performed by the Royal United Services Institute, an independent think tank, was commissioned by then-Deputy Prime Minister Nick Clegg. The reports unanimously concluded that the regulations on the interception of communications were unsatisfactory [40, p. 103; 39, pp. 258 and 285 et seq.; 41, pp. xi and 105 et seq.]. With regard to mass interception of data besides a major overhaul of the system of warrants, all but the ISC called for judicial pre-authorization [41, pp. 108-112]. Concerning the oversight by the IPT, they urged more openness and a domestic appeals chamber [40, p. 116; 39, p. 305; 42, pp. 112 et seq.]. Nevertheless, neither of the reviewers questioned the extensive powers of the intelligence services themselves.

In the meantime, the newly strengthened Conservative government has prepared a draft Investigatory Powers Bill (IPB) [43] and promised a modernized legal regime. Yet, the bill includes even further powers for the intelligence services. The proposal is largely seen as expanding the powers of intelligence services to intercept communication on mass-scale [43, 44]. The interception of external communications as currently governed by Section 8(4) and (5) RIPA is remodelled as Bulk Warrants under Part 6 IPB. Yet, the material scope – except for a slight shift of scope for the purpose of the economic well-being of the UK, which is now only met were it relates to persons outside the UK according to Section 107(2)(a) and (3) IPB – is of the same broad scope as it is under RIPA. The safeguards clauses of Sections 117 and 119 IPB are

[2] For a comprehensive assessment of this proposal cf. Greer, S., Slowe, R.: The Conservative's proposal for a British Bill of Rights: Mired in Muddle, Misconception and Misrepresentation, European Human Rights Law Review 4, 370-381 (2015).

equally vague and make restrictions subject to their necessity as judged by the Secretary of State. Further, the government did not opt for a judicial pre-authorization of warrants. Instead, they are still issued by the Secretary of State under Section 107 IPB and have to be approved by a Judicial Commissioner according to Section 109 IPB. The standard of review to be applied has been subject to concerns, as the bill does not ensure that the Commissioners apply a strict approach [45]. However, the IPB includes a right to appeal for decisions of the IPT in Section 180 IPB. These appeals are lodged with the Court of Appeal in lieu of specific regulations. As has been demonstrated by the High Court, the general courts may be more aware of the human rights dimensions of cases than the specialised IPT. Thus, this provision is an improvement of the status quo.

Nevertheless, in a recent report, the Intelligence and Security Committee of Parliament voiced serious concerns over the draft Bill, which it found disappointing as it did not cover the powers of the intelligence services, but rather left them scattered in various pieces of legislation [46]. Further, the committee harshly criticised the provisions for an inconsistent protection of privacy and its authorisations for the intelligence services, which were too broad and vague. It concluded that the legislation "suffered from a lack of sufficient time and preparation" [46, p. 2].

7 Conclusions

While the IPT's judgment was lauded by some as a victory of privacy rights, this assessment has to be seen critically. The judicial reconditioning of the Snowden revelations before the Tribunal competent to protect the human rights of individuals against government invasions of privacy has had no lasting effect on the ways the intelligence services operate. Luckily, the ECtHR will have a chance to remedy the failures of the IPT and conduct a proper examination and evaluation of GCHQ's activities. While it is hardly possible to predict the outcome of these proceedings, they have an intrinsic value to themselves: external oversight over a system that has more than once been described as opaque.

Regarding the reviews and the reform process initiated in the United Kingdom itself, caution has to be exercised. It appears as though the consequences of the revelations of mass surveillance are to further tighten the grip of intelligence services on online communications. Any efforts to expand the already over-stretched competences of intelligence services should, in turn, be closely monitored.

Further, the new legislation may also have an impact on the outcome of the proceedings before the ECtHR. It may provide the government with a convenient avenue to escape any criticism: the ECtHR will be concerned only with the compatibility of RIPA with the ECHR. If the court finds a violation of the Convention, the government can point to the new legislation. However, as the assessment of the IPB has shown, that would merely be a distraction, as the new regime of secret surveillance contains no limitation as to the points in question before the ECtHR. Additionally, although the judgments of the court are generally only effective inter partes according to Art. 46(1) ECHR, i.e. it is binding only between the parties involved in the case at

hand, it is the function of the court according to Art. 32(1) ECHR to interpret the rights of the Convention. If it finds a violation of the Convention by a certain measure, this extends also to similar measures. Nevertheless, with the now clarified jurisprudence on access to the ECtHR in cases of secret surveillance in *Zakharov*, the court has opened the door for future litigation concerning the IPB as soon as it becomes the law.

References

1. Greenwald, G.: NSA Prism program taps in to user data of Apple, Google and others. The Guardian, 7 June 2013, http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data?guni=Article:in%20body%20link
2. Hopkins, N.: UK gathering secret intelligence via covert NSA operation. The Guardian, 7 June 2013, http://www.theguardian.com/technology/2013/jun/07/uk-gathering-secret-intelligence-nsa-prism
3. MacAskill, E., Borger, J., Hopkins, N., Davies, N., Ball, J.: GCHQ taps fibre-optic cables for secret access to world's communications. The Guardian, 21 June 2013, http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa
4. Chrisafis, A.: France 'runs vast electronic spying operation using NSA-style methods'. The Guardian, 6 July 2013, http://www.theguardian.com/world/2013/jul/04/france-electronic-spying-operation-nsa
5. Überwachung: BND leitet massenhaft Metadaten an die NSA weiter. Der Spiegel, 3 August 2013, http://www.spiegel.de/netzwelt/netzpolitik/bnd-leitet-laut-spiegel-massenhaft-metadaten-an-die-nsa-weiter-a-914682.html
6. Mascolo, G., Goetz, J., von Osten, D.: Zusammenarbeit zweier Geheimdienste – Codename „Eikonal“. Tagesschau, 3 October 2014, https://www.tagesschau.de/inland/bnd-nsa-datenweitergabe-101.html
7. IPT: Liberty and Others v. GCHQ and Others, Case Nos IPT/13/77/H, IPT/13/92/CH, IPT/13/168-173/H, IPT/13/194/CH, IPT/13/204/CH, Judgment of 5 December 2014
8. IPT: Liberty and Others v. GCHQ and Others, Case Nos IPT/13/77/H, IPT/13/92/CH, IPT/13/168-173/H, IPT/13/194/CH, IPT/13/204/CH, Judgment of 6 February 2015
9. IPT: Liberty and Others v. GCHQ and Others, Case Nos IPT/13/77/H, IPT/13/92/CH, IPT/13/168-173/H, IPT/13/194/CH, IPT/13/204/CH, Order of 6 February 2015
10. IPT: Liberty and Others v. GCHQ and Others, Case Nos IPT/13/77/H, IPT/13/92/CH, IPT/13/168-173/H, IPT/13/194/CH, IPT/13/204/CH, Determination of 22 June 2015
11. ECtHR: Big Brother Watch and others v. the United Kingdom, App. no. 58170/13, Statement of Facts of 9 January 2014 (pending)

12. ECtHR: Bureau of Investigative Journalism and Alice Ross v. the United Kingdom, App. no. 62322/14, Statement of Facts of 5 January 2015 (pending)
13. ECtHR: Zakharov v. Russia, App. No. 47143/06, Judgment of 4 December 2015
14. Marauhn, T., Thorn, J.: Kapitel 16: Privat- und Familienleben. In: Dörr, O. et al. (eds.) EMRK/GG Konkordanzkommentar. Vol. I, 2nd edn. Mohr Siebeck, Tübingen (2013)
15. ECtHR: Klass and others v. Germany, App. no. 5029/71, Judgment of 6 September 1978
16. ECtHR: Malone v. the United Kingdom, App. no. 8691/79, Judgment of 2 August 1984
17. Grabenwarter, C., Pabel, K.: Europäische Menschenrechtskonvention. 5th edn. Beck, Munich (2012)
18. ECtHR: Leander v. Sweden, App. no. 9248/81, Judgment of 26 March 1987
19. ECtHR: Bykov v. Russia, App. no. 4378/02, Judgment of 10 March 2009
20. ECtHR: Rotaru v. Romania, App. no. 28341/95, Judgment of 4 May 2000
21. ECtHR: Weber and Saravia v. Germany, App. no. 54934/00, Decision of 29 June 2006
22. ECtHR: Szabo and Vissy v. Hungary, App. no. 37138/14, Judgment of 12 January 2016
23. CJEU: Joined Cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and Others, Judgment of 8 April 2014, EU:C:2014:238
24. Hörnle, J.: How to control interception-does the UK strike the right balance?. 26 Computer Law & Security Review 26, 649–658 (2010)
25. Vaniaio, N., Miettinen, S.: Telecommunications data retention after Digital Rights Ireland: legislative and judicial reactions in the Member States. International Journal of Law and Information Technology, advance access (2015)
26. Kühling, J., Heitzer, S.: Returning through the National Back Door? The Future of Data Retention after the ECJ Judgment on Directive 2006/24 in the UK and Elsewhere. European Law Review 40, 263-278 (2015)
27. Emergency surveillance bill clears Commons, The Guardian, 16 July 2014, http://www.theguardian.com/world/2014/jul/16/emergency-surveillance-bill-clears-commons
28. Smith, G.: Dissecting DRIP - the emergency Data Retention and Investigatory Powers Bill. Cyberleagle, 12 July 2014, http://cyberleagle.blogspot.co.uk/2014/07/dissecting-emergency-data-retention-and.html
29. High Court of Justice, Queen's Bench Division: R. (on the application of Davis and others) v. Secretary of State for the Home Department and others. Case No: CO/3665/2014, CO/3667/2014, CO/3794/2014, Judgment of 17 July 2015
30. CJEU: Case C-698/15 Davis and Others, Order of 1 February 2016, EU:C:2016:70
31. Privacy International: GCHQ-NSA intelligence sharing unlawful, says UK surveillance tribunal. Press Release, 6 February 2015, https://www.privacyinternational.org/node/482

32. Liberty: GCHQ intercepts communications of human rights groups. Press Release, 22 June 2015, https://www.liberty-human-rights.org.uk/news/press-releases-and-statements/gchq-intercepts-communications-human-rights-groups
33. Wheelhouse, A.: The Legality of Mass Surveillance Operations. Oxford Human Rights Hub Blog, 7 February 2015, http://ohrh.law.ox.ac.uk/the-legality-of-mass-surveillance-operations/
34. ECtHR: Burden v. the United Kingdom, App. no. 13378/05, Judgment of 29 April 2008
35. ECtHR: 10 Human Rights Organisations and Others v. the United Kingdom, App. no. 24960/15, Statement of Facts of 24 November 2015 (pending)
36. ECtHR: Delfi AS v. Estonia, App. no. 64569/09, Judgment of 16 June 2015
37. Watt, N., Mason, R.: Cameron 'committed to breaking link with European court of human rights'. The Guardian, 1 June 2015, http://www.theguardian.com/law/2015/jun/01/david-cameron-european-court-of-human-rights
38. Conservative Party: Protecting Human Rights in the UK. p. 5, London (2014), https://www.conservatives.com/~/media/files/downloadable%20Files/human_rights.pdf
39. ECtHR, Camenzid v. Switzerland, App. no. 21353/93, Judgment of 16 December 1997
40. Intelligence and Security Committee of Parliament: Privacy and Security: A modern and transparent legal framework. London (2015), https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20150312_ISC_P%2BS%2BRpt%28web%29.pdf?attachauth=ANoY7coGhW2Ehaqy1VRIMKAhsgXIb65gbZ6rLs0Z-yEiA0U_T-MyF1wV0RDdlyhG1CgLsM0h-fG3-7rVVgSsdANXhuNtSXcx_61IPJOEWFSbh0usafUjfcDVtGmGIwNA3vHGC0-ZJoJdXUq6x-tFgC4k8EKt9HqH9OiOd6l1qCfbyM1dpn_JNfQ8RxcskFMz0ndA5qwcxUsuOhuW2LbIBqEQ5B6uFAr9zYvSKu4FLjWV0LjcYOF3TDvig6xDwjMTebxEY3o7t_RD&attredirects=1
41. Anderson, D.: A Question of Trust, London (2015), https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Print-Version.pdf
42. Royal United Services Institute for Defence and Security Studies: A Democratic Licence to Operate. London (2015), https://www.rusi.org/downloads/assets/ISR-Report-press.pdf
43. Draft Investigatory Powers Bill, November 2015, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473770/Draft_Investigatory_Powers_Bill.pdf
44. Wheelhouse, A.: The Investigatory Powers Bill: A (Somewhat) Different Balance Between Privacy and Security. Oxford Human Rights Hub Blog, 25 November 2015, http://ohrh.law.ox.ac.uk/the-investigatory-powers-bill-a-somewhat-different-balance-between-privacy-and-security/

45. Travis, A., MacAskill, E.: Theresa May unveils UK surveillance measures in wake of Snowden claims: The Guardian, 4 November 2015, http://www.theguardian.com/world/2015/nov/04/theresa-may-surveillance-measures-edward-snowden
46. Murphy, C. C., Simonsen, N.: It's time to overhaul the Investigatory Powers Bill. UK Human Rights Blog, 11 February 2016, http://ukhumanrightsblog.com/2016/02/11/its-time-to-overhaul-the-investigatory-powers-bill/
47. Intelligence and Security Committee of Parliament: Report on the draft Investigatory Powers Bill. London (2016), https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20160209_ISC_Rpt_IPBill%28web%29.pdf?attachauth=ANoY7cpPzZp9EmENG7bQZEi_c310A6r-dV_L-_m7w8jBnmE_H4c8yPpEL5fgJkiGeulmYn8wPnwI27SAgHov7XyAZUnJEKxHFoYiN13baQgUkXIwfp_aC-Us9pM0d0-o_ToLfJkniTRluNbsvvDI--q2vMmbYbegA_muG4gB94Zsb4KY4lrdEQdshu191DnE0C7V9Qlz1dAJrYj4xEQaGxuZ2nly9Sy8bopaSa7in7Fo71KBCdhjVKDhP4lQi_OfJaCTR6vlrhh9&attredirects=0