

## IN THE EUROPEAN COURT OF HUMAN RIGHTS

Application No. 58170/13

**Big Brother Watch and others v. the United Kingdom**

### WRITTEN COMMENTS OF THE OPEN SOCIETY JUSTICE INITIATIVE

1. These written comments are intended to assist the Court in clarifying the international obligations on Council of Europe Member States to respect the right to private and family life, including freedom of communication, when they use secret surveillance technologies to intercept and process vast quantities of personal data in bulk.<sup>1</sup>
2. The applicants allege that the UK government has violated Article 8 through (a) its own TEMPORA programme, under which the Government Communications Headquarters (GCHQ) accesses external communications passing along fibre-optic cables running between the UK and North America,<sup>2</sup> and (b) its receipt of internet communications gathered by the US under its PRISM programme. Both programmes allow the UK to acquire in bulk both the content of communications as well as metadata. The applicants claim that these activities violate Article 8 because the legal systems that regulate those activities are not in accordance with law, necessary and proportionate, and lack required safeguards.
3. While there is no formal definition of “bulk interception” under international law, it refers to techniques used by a government to gather and process data on a large scale, even if it is only a small proportion of the total, that are primarily carried over international fibre-optic cables.<sup>3</sup> These data include the *content* of communications such as emails, telephone calls, social media posts and web-based chat services, as well as the acquisition of *metadata* (also referred to as “communications data”).<sup>4</sup>
4. The term “bulk interception” has been used to refer to a range of practices, leading to varying conclusions regarding its legality. This may include the gathering and processing of a significant volume of data (both content and metadata) to capture and identify communications containing data about unlawful activities, or of persons individually suspected to be engaged in them, as well as data of persons about whom there is no individualised suspicion. In its extreme, bulk interception refers to the open-ended collection of all accessible data, without any suspicion-based targeting. The secrecy of many programs which engage in these practices significantly inhibits their precise description.
5. While the Court has a rich case law on Article 8 obligations relating to surveillance, this case raises new issues arising from advances in both communications and surveillance technologies, that have together greatly expanded the capability of the State to intercept and process vast quantities of personal data.
6. These written comments will address:

---

<sup>1</sup> For purposes of this submission, the “process[ing]” of data refers to the search, analysis, dissemination, storage, and destruction of intercepted data.

<sup>2</sup> “External communication” means a communication sent or received outside the British Islands, as defined by the UK Regulation of Investigatory Powers Act 2000 (RIPA) Section 20.

<sup>3</sup> This definition is adapted from the UK’s Intelligence and Security Committee of Parliament, “Privacy and Security: A modern and transparent legal framework,” 12 March 2015, para. 126, and footnote 2.

<sup>4</sup> The term “metadata” (synonymous with “communications data”) is explained in the Witness Statement of Ian Brown, 27 September 2013, para. 31 (Metadata is “‘data about the data’ i.e. data recording the means of creation of transmitted data, the time and date of its creation, its creator, the location on a computer network where it was created and the standards used.”).

- *A. Metadata and the Right to Privacy.* The bulk interception and processing of metadata by the State interferes with Article 8.
- *B. Preconditions for Bulk Interception.* If bulk interception can ever be lawful, States must ensure that (a) the governing law is sufficiently precise, (b) the scope of the information gathered is restricted by time and geography, and (c) that information may only be gathered (i.e. prior even to it being processed) on the basis of reasonable suspicion and strict necessity. There must also be other safeguards that are not covered in this submission. If it is the Court’s view that these preconditions effectively strip bulk interception of its defining character, then there is good reason to regard bulk interception as *per se* unlawful.
- *C. Additional Safeguards for Receiving and Requesting Third-Party Intercepts.* In addition to the preconditions that apply to States carrying out bulk interception, safeguards must also be put in place to ensure States do not circumvent individuals’ Article 8 rights when receiving and requesting foreign State intercepts.

#### **A. METADATA INTERCEPTION AND COLLECTION INTERFERES WITH THE RIGHT TO PRIVACY**

7. While the Court has analysed in depth the different ways interception and subsequent processing of *content data* interferes with Article 8,<sup>5</sup> international human rights law also recognises that the interception and processing of *metadata* can be just as intrusive as that of content-based data. The Court should therefore apply its content-based Article 8 assessments to affirm that metadata interception and processing interferes with Article 8.
8. Even prior to the widespread use of the internet and the interception of metadata, this Court considered more limited examples of what we would today consider metadata under the term “metering data,” and found that the interception even of this more limited form of communications constituted an interference with Article 8. In the 1984 case *Malone v. UK*, in response to the UK’s argument that “metering data” (in that case numbers dialled and duration of calls) did not interfere with Article 8 because it did not contain content, the Court noted that it “does not accept... that the use of data obtained from metering, whatever the circumstances and purposes, cannot give rise to an issue under Article 8.”<sup>6</sup> The Court observed that the numbers dialled were an “integral element in the communications made by telephone” and the handing over of that information from a telephone service provider to the police without the consent of the subscriber amounted to an interference with a right guaranteed by Article 8.<sup>7</sup>
9. The UN High Commissioner on Human Rights has stated the collection and retention of metadata “amounts to an interference with privacy whether or not those data are subsequently consulted or used.”<sup>8</sup> The UN Special Rapporteur on human rights and terrorism has stated the same.<sup>9</sup> The European Parliament’s Committee on Civil Liberties, Justice and Home Affairs has recognized that the collection of metadata, like content data, permits States to gather vast quantities of information about nearly all aspects of an individual’s private life. In its 2014 report on surveillance, the Committee noted:

---

<sup>5</sup> While not exhaustive, this includes assessing content data through its *interception per se* (*Weber and Saravia v. Germany*, Admissibility Decision of 29 June 2006, para. 79), *storage* (*Amann v. Switzerland*, Judgment of 16 February 2000, para. 69; and *Liberty v. U.K.*, Judgment of 1 July 2008, para. 57), *transmission* (*Weber and Saravia v. Germany*, Admissibility Decision of 29 June 2006, para. 79); and *destruction* (*S. and Marper v. U.K.*, Judgment of 4 December 2008, para. 99; *Liberty and others v. U.K.*, Judgment of 1 July 2008, para. 69.)

<sup>6</sup> *Malone v. U.K.*, Judgment of 2 August 1984, para. 84.

<sup>7</sup> *Ibid.*, paras. 84 and 87.

<sup>8</sup> Office of the United Nations High Commissioner for Human Rights, “Report on the right to privacy in the digital age,” A/HRC/27/37, 30 June 2014, para. 20.

<sup>9</sup> UN Special Rapporteur on human rights and terrorism, Ben Emmerson, “Report on the promotion and protection of human rights and fundamental freedoms while countering terrorism,” A/69/397, 23 September 2014, para 55.

“By being able to collect data regarding the content of communications, *as well as metadata*, and by following citizens’ electronic activities, in particular their use of smartphones and tablet computers, intelligence services are de facto able to know almost everything about a person.”<sup>10</sup>

10. The Inter-American Court of Human Rights has also determined that the collection of metadata, and not just content, interferes with the right to privacy. In the case of *Escher v. Brasil*, the Court stated that the right to privacy “applies to telephone conversations irrespective of their content” and can include the collection of information about “the destination or origin of the calls that are made... [and] the frequency, time and duration of the calls.”<sup>11</sup>
11. The 23 January 2014 report of the Privacy and Civil Liberties Oversight Board (PCLOB), an independent agency within the executive branch of the United States government, similarly concluded that telephone metadata, similar to the content of telephone calls, may be “highly revealing” of deeply personal aspects of an individual’s life.<sup>12</sup> The PCLOB gave several illustrative examples, such as “calling a suicide prevention hotline;...calling an HIV testing service, then one’s doctor, then one’s health insurance company within the same hour; ...and calling one’s gynaecologist, speaking for half an hour, then calling the local Planned Parenthood number later that day.”<sup>13</sup> The PCLOB ultimately concluded: “[T]elephone metadata is information about a person’s conduct.... When the government collects metadata about its citizens, therefore, it is collecting information about its citizens’ activity.”<sup>14</sup> The United States Court of Appeals for the Second Circuit also recognized that the collection of metadata raises serious privacy concerns because “[m]etadata can reveal civil, political, or religious affiliations; they can also reveal an individual’s social status, or whether and when he or she is involved in intimate relationships.”<sup>15</sup>

## **B. PRECONDITIONS FOR BULK INTERCEPTION**

12. Bulk interception is a particularly serious interference with the right to privacy that, due to its untargeted, invasive, and widespread nature,<sup>16</sup> requires enhanced preconditions and other safeguards to ensure that it is done in accordance with the law and only when strictly necessary. As the Court has noted, in response to technological advancements and “massive monitoring of communications”<sup>17</sup> the “guarantees required by the extant Convention case-law on interceptions need to be enhanced so as to address the issue of such surveillance practices.”<sup>18</sup> The Grand

---

<sup>10</sup> European Parliamentary Assembly Committee on Civil Liberties, Justice and Home Affairs, “Report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens’ fundamental rights and on transatlantic cooperation in Justice and Home Affairs (2013/2188(INI)),” 21 February 2014, Explanatory Statement (emphasis added).

<sup>11</sup> *Escher v. Brasil*, IACtHR, Preliminary Objections, Merits, Reparations and Costs, Judgement of 6 July 2009, Series C No. 200, para. 114.

<sup>12</sup> Privacy and Civil Liberties Oversight Board, “Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court,” 23 January 2014 (“PCLOB, January 2014 Report”), p. 132.

<sup>13</sup> *Ibid.*, p. 157.

<sup>14</sup> *Ibid.*

<sup>15</sup> *ACLU v. Clapper*, US Court of Appeals for the Second Circuit, 7 May 2015, p. 9. Similarly, the United States Federal District Court concluded that available surveillance technologies and expansive ways in which people use telecommunications services “now reveal an entire mosaic—a vibrant and constantly updating picture of the persons’ life.” *Klayman v. Obama*, US District Court for DC, 16 December 2013, p. 54.

<sup>16</sup> See *Szabó and Vissy v. Hungary*, Judgment of 12 January 2016, paras. 68, 70, and 73. The CJEU and an Advocate General have also noted that when data collection’s interference on the right to privacy is “wide-ranging”—as is the case with bulk interception—it “must be considered to be particularly serious.” CJEU, Joined Case (C-293/12 and C-594/12), *Digital Rights Ireland Ltd.*, Judgment of 8 April 2014, para. 37; CJEU Advocate General C-362/14), *Maximillian Schrems v. Data Protection Commissioner*, Opinion of 23 September 2015 (1), para. 171.

<sup>17</sup> *Szabó and Vissy v. Hungary*, Judgment of 12 January 2016, para. 68.

<sup>18</sup> *Ibid.*, para. 70. See also, para. 68.

Chamber of the Court of Justice of the European Union (CJEU) has noted in a similar context that “the need for such safeguards is all the greater where...personal data are subjected to automatic processing and where there is a significant risk of unlawful access to those data.”<sup>19</sup>

### **Bulk Interception is a Particularly Serious Interference with Privacy**

13. The amount of data available for interception today, as well as government appetite for data and ability to obtain it, far exceeds what was possible in the past, including when *Malone v. UK* or *Weber and Saravia v. Germany* were lodged in 1978 and 1995 respectively.<sup>20</sup> In particular, the untargeted, invasive, and widespread nature of bulk interception makes it a “particularly serious” interference<sup>21</sup> with the individual’s right to privacy and “in view of the risk that a system of secret surveillance for the protection of national security may undermine or even destroy democracy under the cloak of defending it.”<sup>22</sup>
14. In further recognition of the dangers posed by broad surveillance powers, the Court has contrasted situations where “the impugned legislation did not allow for ‘indiscriminate capturing of vast amounts of communications’” with those where “broad-based provisions ... can be taken to enable so-called strategic, large-scale interception, which is a matter of serious concern”, finding a violation of Article 8 on the basis that, in part, the latter allowed for surveillance without the need for suspicion.<sup>23</sup>
15. Other legal authorities have criticized bulk interception for its indiscriminate surveillance of individuals with no link to the intended purpose of the surveillance. The CJEU Grand Chamber found that the Data Retention Directive (2006/24) did not meet the requirement of necessity under EU law because, in part, the provisions applied “even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime.”<sup>24</sup>
16. CJEU Advocate General Bot, in his assessment of whether EU Member States could transfer data to the United States, was similarly critical of limitless (or untargeted) data collection. He held that “mass, *indiscriminate* surveillance is inherently disproportionate and constitutes an unwarranted interference with the rights guaranteed by Articles 7 and 8 of the Charter.”<sup>25</sup> Advocate General Bot described this practice as one that permits access to, “in a comprehensive manner, all persons using electronic communications services, without any requirement that the persons concerned represent a threat to national security” and that it does so “without any

---

<sup>19</sup> CJEU, Joined Case (C-293/12 and C-594/12), *Digital Rights Ireland Ltd.*, Judgment of 8 April 2014, para. 55.

<sup>20</sup> *Malone v. U.K.*, Judgment of 2 August 1984; *Weber and Saravia v. Germany*, Admissibility Decision of 29 June 2006. For increase in surveillance and data collection see, Fred H. Cate, James X. Dempsey and Ira S. Rubinstein, “Systematic government access to private-sector data”, *International Data Privacy Law*, vol. 2, No. 4, 2012, p. 195; Witness Statement of Ian Brown, 27 September 2013, paras. 7-8; Office of the United Nations High Commissioner for Human Rights, “Report on the right to privacy in the digital age,” A/HRC/27/37, 30 June 2014, para. 2; General Assembly, Resolution 68/167, 18 December 2013, Preamble; and CJEU, Advocate General (C-293/12), *Digital Rights Ireland Ltd v The Minister for Communications, Marine and Natural Resources, The Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána Ireland and The Attorney General*, Opinion of 12 December 2013 (1), para. 73.

<sup>21</sup> The CJEU and an Advocate General have noted that when data collection’s interference on the right to privacy is “wide-ranging”—as is the case with bulk interception—it “must be considered to be particularly serious.” CJEU, Joined Case (C-293/12 and C-594/12), *Digital Rights Ireland Ltd.*, Judgment of 8 April 2014, para. 37; CJEU Advocate General C-362/14), *Maximillian Schrems v Data Protection Commissioner*, Opinion of 23 September 2015 (1), para. 171. See, also, *Szabó and Vissy v. Hungary*, Judgment of 12 January 2016, para. 68, 70, and 73.

<sup>22</sup> *Szabó and Vissy v. Hungary*, Judgment of 12 January 2016, para. 57.

<sup>23</sup> *Ibid.*, para. 69; contrasting *Kennedy v. U.K.*, Judgment of 18 May 2010, para. 160.

<sup>24</sup> CJEU, Joined Case (C-293/12 and C-594/12), *Digital Rights Ireland Ltd.*, Judgment, 8 April 2014, para. 58.

<sup>25</sup> CJEU Advocate General C-362/14), *Maximillian Schrems v. Data Protection Commissioner*, Opinion, 23 September 2015 (1), para. 200 (emphasis added).

differentiation, limitation or exception according to the objective of general interest pursued.”<sup>26</sup> The High Court of Ireland, which referred the case to the CJEU, was similarly critical of “mass and undifferentiated” data access.<sup>27</sup> The CJEU Grand Chamber found that “legislation permitting the public authorities to have access on a *generalized basis* to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life.”<sup>28</sup>

17. The European Parliament has also expressed concern about the use of bulk surveillance against large portions of a community, which necessarily captures many innocent individuals. The first main finding of its 2014 European Parliament resolution (2013/2188(INI)) was that the collection, storage, and analysis of “communication data, including content data, location data and metadata of all citizens around the world” were being done on an “unprecedented scale and in an *indiscriminate and non-suspicion-based manner*.”<sup>29</sup> According to the report, this activity was “leading to every citizen being treated as a suspect and being subject to surveillance.”<sup>30</sup> The report specifically condemned “the vast and systemic blanket collection of the personal data of *innocent people*, often including intimate personal information.”<sup>31</sup> The European Commission for Democracy through Law (Venice Commission) has also noted that strategic surveillance “does not necessarily start with a suspicion against a particular person or persons” and thus poses a risk for individual rights.<sup>32</sup>
18. The Council of Europe’s Commissioner for Human Rights has been particularly critical of the untargeted nature of bulk interception. In a 2014 Issue Paper on the rule of law and the Internet, the Commissioner stated that “[s]uspicionless mass retention of communications data is fundamentally contrary to the rule of law.”<sup>33</sup> The Commissioner also supported the claim that “[c]ompulsory, suspicionless, untargeted retention of communication records ‘just in case’ the data might be useful in some future police or secret service enquiry ... ought to be viewed as mass surveillance of citizens without due cause: a fundamental departure from a basic principle of the rule of law.”<sup>34</sup>
19. In the United States, the PCLOB has also raised serious concerns about the harm that bulk interception poses to privacy and democracy. In its criticisms of the US’s sweeping metadata collection programme, the PCLOB said it was untenable for a system of professed limited government to argue that just because any record *may* be relevant to issues of national security that *all* records *must* be collected, mirroring the Court’s objection to laws that attempt to account for “every eventuality”.<sup>35</sup>
20. The PCLOB explained that the programme’s safeguards on the *use* of the collected information “cannot fully ameliorate the implications for privacy, speech, and association that follow from the government’s ongoing *collection* of virtually all telephone records of every American.”<sup>36</sup>

---

<sup>26</sup> *Ibid.*, 198-199.

<sup>27</sup> High Court of Ireland, *Schrems v. Data Protection Commissioner*, 18 June 2014, para. 52.

<sup>28</sup> CJEU, Case (C-362/14), *Maximillian Schrems v. Data Protection Commissioner*, Judgment, October 2015, para. 94 (emphasis added).

<sup>29</sup> European Parliament resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens’ fundamental rights and on transatlantic cooperation in Justice and Home Affairs (2013/2188(INI)), para. 1 (emphasis added).

<sup>30</sup> *Ibid.*, para. F. (emphasis added).

<sup>31</sup> *Ibid.*, 10 (emphasis added).

<sup>32</sup> European Commission for Democracy through Law (Venice Commission), “Update of the 2007 report on the democratic oversight of the security services and report on the democratic oversight of signals intelligence agencies”, CDL-AD(2015)006, March 2015, para. 51.

<sup>33</sup> Council of Europe Commissioner for Human Rights, “The rule of law on the Internet and in the wider digital world” (Issue Paper), December 2014, p. 22.

<sup>34</sup> *Ibid.*, p. 115.

<sup>35</sup> *S. and Marper v. U.K.* Judgment of 4 December 2008, para. 96.

<sup>36</sup> PCLOB, January 2014 Report, p. 155-156 (emphasis added).

They noted that “permitting the government to routinely collect the calling records of the entire nation fundamentally shifts the balance of power between the state and its citizens.”<sup>37</sup>

21. The PCLOB also objected to any justification of the programme based on the notion that “all records become relevant to an investigation...because the government has developed an investigative tool that functions by collecting all records to enable later searching.” The PCLOB noted that such reasoning quickly erodes any limited powers on government surveillance because “the implication of this reasoning is that if the government develops an effective means of searching through *everything* in order to find *something*, then *everything* becomes relevant to its investigations.”<sup>38</sup>
22. Bulk interception must be assessed in light of its increasingly real and potential interference on other rights such as freedom of expression and association, including through its “chilling effect,” and by intercepting communications protected under domestic and international law.<sup>39</sup> These factors, whether considered separately or cumulatively, dramatically increase the interference that bulk interception programmes can have on society and heighten the need for enhanced preconditions and safeguards.

### **Necessary Preconditions for Bulk Interception**

23. For a bulk interception program, however so defined, to be lawful it must satisfy several preconditions, together with other safeguards that are not covered in this submission, in order that it is conducted in accordance with the law and is strictly necessary, so as to avoid abuse and arbitrary interference by government authorities.<sup>40</sup> These preconditions include (a) that the governing law must be sufficiently precise, (b) that the scope of the information gathered must be restricted by time and geography, and (c) that information may only be gathered (i.e. prior even to it being processed) on the basis of reasonable suspicion, and by subjecting the proposed surveillance to an *ex ante* evaluation of strict necessity. If such preconditions are not put in place, the government may have unfettered powers<sup>41</sup> and individuals with no links to prohibited behaviour would have to cease nearly all use of electronic communications to protect their right to privacy. Under such circumstances, bulk interception amounts to limitless, open-ended collection of all accessible data, without any suspicion-based targeting, which is *per se* unlawful.
24. *Precision*. In general, the Court requires that laws are “formulated with sufficient precision to enable any individual – if need be with appropriate advice – to regulate his conduct.”<sup>42</sup> This ensures the individual “adequate protection against arbitrary interference,”<sup>43</sup> and that its strict necessity can be evaluated and justified.<sup>44</sup> More specifically, the Court has held that “tapping and other forms of interception of telephone conversations constitute a serious interference with private life and correspondence and must accordingly be based on a ‘law’ that is particularly

---

<sup>37</sup> *Ibid.*, p. 156.

<sup>38</sup> *Ibid.*, p. 62.

<sup>39</sup> For example, attorney-client privileged information, human rights complaints, and other forms of protected communication. See, e.g., Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, “Report on implications of States’ surveillance of communications on the exercise of the human rights to privacy and to freedom of opinion and expression,” A/HRC/23/40, 17 April 2013, paras. 24, 49, and 52; American Civil Liberties Union and Human Rights Watch, “With Liberty to Monitor: All How Large-Scale US Surveillance is Harming Journalism, Law, and American Democracy,” July 2014; and PEN, “Global Chilling: The Impact of Mass Surveillance on International Writers” (Results from PEN’s International Survey of Writers), 5 January, 2015. See, also, Venice Commission Report, March 2015, paras. 18, 62, and 95.

<sup>40</sup> See, for example, *Zakharov v. Russia*, Judgment of 4 December 2015, para. 227.

<sup>41</sup> *Zakharov v. Russia*, Judgment of 4 December 2015, para. 230.

<sup>42</sup> *Amann v. Switzerland*, Judgment of 16 February 2000, paras. 55 and 56.

<sup>43</sup> *Szabó and Vissy v. Hungary*, Judgment of 12 January 2016, para. 65.

<sup>44</sup> See, *Gillan and Quinton v. UK*, Judgment of 12 January 2010, para. 80; *Colon v. Netherlands*, Judgment of 15 May 2012, para. 85.

precise.”<sup>45</sup> The Court further explained, “It is essential to have clear, detailed rules on the subject, especially as the technology available for use is continually becoming more sophisticated.”<sup>46</sup> The Court has also stated that the level of precision required of domestic legislation “cannot in any case provide for every eventuality,”<sup>47</sup> which is ultimately what limitless bulk interception does.

25. *Scope*. In the context of telephone and other communications surveillance, the Court has found that the necessary “minimum safeguards” to avoid an abuse of power should include “the definition of the categories of people liable to have their telephones tapped” together with temporal limitations of the surveillance.<sup>48</sup> The Court has emphasized that “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 been committed... [and which do] not mention the duration for which interception is authorised... grant a very wide discretion to the law-enforcement authorities as to which communications to intercept, and for how long.”<sup>49</sup> These, along with other shortcomings, resulted in the Court finding that the “the circumstances in which public authorities are empowered to resort to secret surveillance measures are not defined with sufficient clarity” and the provisions thus “do not provide sufficient guarantees against arbitrary interference.”<sup>50</sup>
26. In determining whether a law properly defines “categories of people,” the Court has assessed the precision of *who* is liable to surveillance and the precision of the *act* for which that person is suspected of being liable.<sup>51</sup> In *Zakharov v. Russia*, the Court found that a failure to be sufficiently precise “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, thereby creating possibilities for abuse.”<sup>52</sup> In *Szabó and Vissy v. Hungary*, the Court was similarly concerned that a law permitting surveillance on a wide range of persons might be “interpreted as paving the way for the unlimited surveillance of a large number of citizens.” The Court pointed out that such a system would have “no requirement of any kind for the authorities to demonstrate the actual or presumed relation between the persons or range of persons ‘concerned’ and the prevention of any terrorist threat.”<sup>53</sup>
27. The CJEU Grand Chamber has also noted that the Data Retention Directive’s lack of temporal and geographic limitations were part of “a general absence of limits” that contributed to its failure.<sup>54</sup> The U.N. Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, has noted in the context of communications surveillance that “[s]afeguards must be articulated in law relating to [*inter alia*] the...scope and duration of the possible measures.”<sup>55</sup>

---

<sup>45</sup> *Amann v. Switzerland*, Judgment of 16 February 2000, para. 56.

<sup>46</sup> *Ibid.*

<sup>47</sup> *S. and Marper v. U.K.*, Judgment of 4 December 2008, para. 96.

<sup>48</sup> *Zakharov v. Russia*, Judgment of 4 December 2015, para. 231.

<sup>49</sup> *Ibid.*, 265.

<sup>50</sup> *Ibid.*, 302.

<sup>51</sup> *Ibid.*, 245-246.

<sup>52</sup> *Ibid.*, 248.

<sup>53</sup> *Szabó and Vissy v. Hungary*, Judgment of 12 January 2016, para. 67.

<sup>54</sup> “[W]hilst seeking to contribute to the fight against serious crime, Directive 2006/24 does not require any relationship between the data whose retention is provided for and a threat to public security and, in particular, it is not restricted to a retention in relation (i) to data pertaining to a particular time period and/or a particular geographical zone and/or to a circle of particular persons likely to be involved, in one way or another, in a serious crime, or (ii) to persons who could, for other reasons, contribute, by the retention of their data, to the prevention, detection or prosecution of serious offences.” CJEU, Joined Case (C-293/12 and C-594/12), *Digital Rights Ireland Ltd.*, Judgment of 8 April 2014, para. 59.

<sup>55</sup> United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, “Report on implications of States’ surveillance of communications on the exercise of the human rights to privacy and to freedom of opinion and expression,” A/HRC/23/40, 17 April 2013, para. 81.

28. *Reasonable Suspicion*. Any surveillance must be on the basis of reasonable suspicion that the person whose data are at issue is engaged in activity which may lawfully give rise to secret surveillance. In *Zakharov v. Russia*, the Court was considering whether an authority was able to verify the necessity of the Article 8 interference. In doing so, the Court emphasized that the authorizing authority “must be capable of verifying the existence of a *reasonable suspicion* against the person concerned, in particular, whether there are factual indications for suspecting that person of planning, committing or having committed criminal acts or other acts that may give rise to secret surveillance measures, such as, for example, acts endangering national security.”<sup>56</sup> Further authorities are set out in the concurring opinion of Judge Albequerque in *Szabó and Vissy v. Hungary*. The CJEU has taken a similar approach, suggesting that for data retention to be lawful there must be a link between the data retained, an individual, and a crime,<sup>57</sup> and that the Data Retention Directive’s lack of suspicion is part of the “general absence of limits”.<sup>58</sup> The CJEU determined that the Data Retention Directive did not meet the requirement of necessity because, in part, it “applies even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime.”<sup>59</sup>
29. The European Parliament in Resolution 2045 (2015) has also emphasized the importance of reasonable suspicion, urging Council of Europe member and observer States to ensure that the collection and analysis of personal data (including metadata) be based either on consent of the person concerned or “following a court order granted on the basis of *reasonable suspicion of the target being involved in criminal activity*.”<sup>60</sup>
30. In his 2014 report, the U.N. Special Rapporteur on human rights and terrorism raised similar concerns when mass data collection programmes do not require a “prior suspicion directed at any particular individual or organization”,<sup>61</sup> explaining, “[s]ince there is no opportunity for an individualized proportionality assessment to be undertaken prior to these measures being employed, such programmes also appear to undermine the very essence of the right to privacy.”<sup>62</sup>
31. Thus, if bulk interception can ever be lawful there must be strict preconditions before it can be authorised, together with *ex post facto* safeguards which are not covered in this submission. If it is the Court’s view that these preconditions effectively strip bulk interception of its defining character, then there is good reason to regard bulk interception as *per se* unlawful.

### C. ADDITIONAL SAFEGUARDS FOR RECEIVING THIRD-PARTY INTERCEPTS

32. States must not receive or request data from a third party in a manner that circumvents individuals’ Article 8 rights. To ensure this, States must put in place safeguards at the point when the information is first gathered (i.e., prior to it being processed). Safeguards are required at this stage because as soon as data is transferred from one State to another, Article 8 is engaged. These safeguards should include (a) prior scrutiny of the human rights record and interception laws and

<sup>56</sup> *Zakharov v. Russia*, Judgment of December 2015, para. 260 (emphasis added). See also *Szabó and Vissy v. Hungary*, Judgment of 12 January 2016, para. 67.

<sup>57</sup> CJEU, Joined Case (C-293/12 and C-594/12), *Digital Rights Ireland Ltd.*, Judgment of 8 April 2014, para. 58.

<sup>58</sup> “[W]hilst seeking to contribute to the fight against serious crime, Directive 2006/24 does not require any relationship between the data whose retention is provided for and a threat to public security and, in particular, it is not restricted to a retention in relation (i) to data pertaining to a particular time period and/or a particular geographical zone and/or to a circle of particular persons likely to be involved, in one way or another, in a serious crime, or (ii) to persons who could, for other reasons, contribute, by the retention of their data, to the prevention, detection or prosecution of serious offences.” *Ibid.*, para. 59.

<sup>59</sup> *Ibid.*, 58.

<sup>60</sup> European Parliamentary Assembly Resolution 2045 (2015), paras. 4 and 19.1 (emphasis added).

<sup>61</sup> UN Special Rapporteur on human rights and terrorism, Ben Emmerson, “Report on the promotion and protection of human rights and fundamental freedoms while countering terrorism,” A/69/397, 23 September 2014, para 55.

<sup>62</sup> *Ibid.*, para. 52.



practices in the foreign State, including a requirement that States refrain from requesting and accepting data from a foreign State which may have been intercepted and processed arbitrarily, and (b) that any sharing arrangements should also be subject to independent, preferably judicial, *a posteriori* oversight to ensure that the safeguards are in place and enforced.

33. In 2015, the Commissioner for Human Rights warned against “the deliberate or accidental use of international intelligence sharing to circumvent the safeguards that would ordinarily apply to the collection of information,” and emphasized that risks that the right to privacy may be breached are “heightened in the context of intelligence sharing relationships that include automated sharing of electronic data and/or integrated systems collecting and storing information gathered by more than one state.”<sup>63</sup> The Venice Commission registered similar concerns in 2007 and again in 2015.<sup>64</sup>
34. In its 2001 report on a global system for the interception of private and commercial communications (ECHELON interception system), a European Parliament committee stated: “It is quite obvious that intelligence services cannot be allowed to circumvent these [Article 8] requirements by employing assistance from other intelligence services subject to less stringent rules. Otherwise, the principle of legality, with its twin components of accessibility and foreseeability, would become a dead letter and the case law of the European Court of Human Rights would be deprived of its substance.”<sup>65</sup>
35. The Court has noted that “[t]he governments’ more and more widespread practice of transferring and sharing amongst themselves intelligence retrieved by virtue of secret surveillance – a practice ... which concerns both exchanges between Member States of the Council of Europe and with other jurisdictions – is yet another factor in requiring particular attention when it comes to external supervision and remedial measures.”<sup>66</sup>
36. *Prior Scrutiny*. The Commissioner for Human Rights has recommended that oversight bodies should “scrutinise the human rights compliance of security service co-operation...through the exchange of information,” including examining “human rights risk assessment and risk-management processes relating to relationships with specific foreign security services and to specific instances of operational co-operation.”<sup>67</sup> The UN Special Rapporteur on terrorism and human rights advocated for safeguards on inter-state intelligence sharing in a Best Practices Study in 2010. States, he said, should put in place agreements to govern data sharing, that such agreements must take into account human rights implications, and that inter-state intelligence sharing arrangements should be subject to oversight. The Special Rapporteur noted in particular that “intelligence received from a foreign entity may have been obtained in violation of international human rights law”<sup>68</sup> and therefore recommended that “[b]efore entering into an intelligence-sharing agreement or sharing intelligence on an ad hoc basis, intelligence services

---

<sup>63</sup> Council of Europe Commissioner for Human Rights, “Democratic and effective oversight of national security services,” May 2015, p. 24.

<sup>64</sup> European Commission for Democracy through Law (Venice Commission), “Report on the democratic oversight of the security services”, CDL-AD(2007)016, June 2007, para. 188; Venice Commission Report, March 2015, para. 78.

<sup>65</sup> European Parliament Temporary Committee on the Echelon Interception System, report on the existence of a global system for the interception of private and commercial communications, A5- 0264/2001, p. 87.

<sup>66</sup> *Szabó and Vissy v. Hungary*, Judgment of 12 January 2016, para. 78.

<sup>67</sup> Council of Europe Commissioner for Human Rights, “Democratic and effective oversight of national security services,” May 2015, p. 12.

<sup>68</sup> UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, “Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight,” A/HRC/14/46, 17 May 2010, para. 47.

undertake an assessment of the counterpart's record on human rights and data protection, as well as the legal safeguards and institutional controls that govern the counterpart."<sup>69</sup>

37. *Oversight*. The Court has called for oversight of such sharing arrangements: "It is in this context that the external, preferably judicial, *a posteriori* control of secret surveillance activities, both in individual cases and as general supervision, gains its true importance."<sup>70</sup> The European Parliament's ECHELON committee sought to safeguard against abuse by insisting that "an intelligence service may seek from one of its counterparts only data obtained in a manner consistent with the conditions laid down in its own national law."<sup>71</sup> The 2014 European Parliament report (see para. 17) also stressed the need for States to "refrain from accepting data from third States which have been collected unlawfully", in violation of European human rights law.<sup>72</sup> The Venice Commission, which also proposed strong oversight on intelligence sharing regimes, emphasized that when a sending State refuses to answer questions about the origins of the data to the oversight mechanisms in the receiving State, the receiving State should be required "to take into account the human rights implications of this transfer/receipt before it takes place, and to mitigate whatever risks might arise as a result of such cooperation." The Venice Commission said this is "a minimum standard which would reconcile security, and human rights concerns."<sup>73</sup>
38. The U.N. Special Rapporteur on human rights and terrorism has also stated that intelligence sharing arrangements should be subject to independent oversight mechanisms, explaining that "[i]ndependent oversight institutions can scrutinize the legal framework and procedural dimensions of intelligence-sharing agreements to ensure that they comply with national laws and relevant international legal standards."<sup>74</sup>

## CONCLUSION

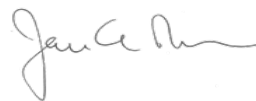
39. European history has witnessed governments repeatedly violate the human rights of their citizens through mass surveillance. In an age of previously unimagined technological advances, it is essential that all Member States of the Council of Europe adhere to strict safeguards in the conduct of surveillance, so as to protect individual rights and maintain the rule of law.

9 February 2016

Jonathan Horowitz, Legal Officer



James A. Goldston, Executive Director



Open Society Justice Initiative

---

<sup>69</sup> *Ibid.*, Practice 33.

<sup>70</sup> *Szabó and Vissy v. Hungary*, Judgment of 12 January 2016, para. 79.

<sup>71</sup> European Parliament Temporary Committee on the Echelon Interception System, report on the existence of a global system for the interception of private and commercial communications, A5- 0264/2001, p. 88.

<sup>72</sup> European Parliament resolution of 12 March 2014, para. 26. The report called on the United States to revise its surveillance legislation in order to bring it into line with international human rights law, para. 31.

<sup>73</sup> Venice Commission Report, June 2007.

<sup>74</sup> UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, "Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight," A/HRC/14/46, 17 May 2010, para. 49.