International cooperation by (European) security and intelligence services: reviewing the creation of a joint database in light of data protection guarantees

Cedric M.J. Ryngaert* and Nico A.N.M. van Eijk**

Key Points

- Increasing multinational cooperation between intelligence and security services, including the establishment of a joint database on (alleged) jihadists, raises legal concerns over the protection of personal data, in particular with respect to the allocation of responsibility among participating states, the geographic scope of fundamental data protection norms, and the applicable law.
- It is argued that states participating in multinational cooperative efforts may share responsibility, eg in relation to a shared database. However, for reasons of proximity, the host state of the server has heightened duties of care.
- It is also argued that where a participating state, in particular the host state, exercises virtual control (jurisdiction) over an individual person's data, such a state has data protection obligations towards that person, regardless of the latter's location.
- Participating states, and again in particular the host state, are under an obligation to put in place adequate control systems, including with a view to preventing the transfer of data that have been gathered by states in breach of data protection guarantees.
- If systemic failures in the multilateral system are identified, states are barred from transferring data to the system, unless they can obtain credible guarantees that data will be adequately protected.
- General principles of data protection law, derived from case law as well as general or sector-specific regulations, govern the processing and transfer of data in the context of multinational intelligence cooperation, including the management of a joint database. There is no reason not to apply them in the context of national security.

Introduction

National intelligence and security services are stepping up their cooperation to address national security threats, in particular terrorism. Given the sensitivity of national security, such cooperation will normally occur on the basis of legally non-binding, informal arrangements rather than 'hard' treaties.[1] Under these arrangements, states scale up the exchange of data concerning persons of interest. Most notably, the Counter Terrorism Group

* Cedric Ryngaert, School of Law, Utrecht University, RENFORCE research programme, The Netherlands

** Nico van Eijk, University of Amsterdam/IVIR, The Netherlands.

Cedric Ryngaert's research has been funded by the European Research Council under the Starting Grant Scheme (Proposal 336230—UNIJURIS) and the Dutch Organization for Scientific Research under the VIDI Scheme (No 016.135.322).The article elaborates on an independent advisory opinion given in 2017 to the CTIVD (supervisor of Dutch intelligence services).

1 Still, these arrangements may be imbued with sufficient political legitimacy, and ultimately be as effective, if not more so, as compared to formal legal cooperation. See on informal international law-making, eg Joost Pauwelyn, Ramses A Wessel and Jan Wouters (eds), *Informal International Lawmaking* (OUP 2012).

(CTG), which consists of the EU Member States plus Norway and Switzerland,[2] has activated a database containing personal data of (alleged) jihadists travelling to, or returning from particular conflict areas. The database is (near) real-time available to all CTG participating services. In 2017, an operational platform was formally opened, which allows for more detailed multilateral consultations. This operational platform is also available to all CTG participating services.[3]

This database is fed by all participating states,[4] but its server is based on the territory of just one of them, in The Netherlands, hosted by the AIVD, the Dutch General Intelligence and Security Service.[5] In terms of set-up, the database somewhat resembles the database established by European police services and managed by Europol.[6]

These developments raise acute questions as to the adequate protection of data by multiple cooperating states, in particular as to the locus of responsibility in case of breach and the required level of data protection. In essence, four legal questions arise: (1) What form of responsibility for data breaches does the non-binding informal cooperation envisaged by the security services yield?; (2) Do the individuals whose data are processed fall within the jurisdiction of the participating states, ie do these states have human rights obligations *vis-à-vis* the individuals concerned, who may well happen to be *outside* the territory?; (3) Under what circumstances is the responsibility of the database manager engaged when he processes deficient data from participating states, and *vice versa*, under what circumstances is the responsibility of a state engaged when it transfers data to a deficient international database?; (4) What substantive guarantees as to the level of data protection and the management of the database need to be provided, and in particular from what legal regime are they to be drawn (the legal regime of the server's host state, an international legal regime . . .)?

This article, which is based on an expert opinion of the authors to the Dutch Review Committee on the Intelligence and Security Services (CTIVD),[7] is relevant for cooperation among all security and intelligence services. Its emphasis, however, lies on the exchange of data between European states, defined here as states that are Contracting Parties to the European Convention on Human Rights (ECHR), or at least the exchange of data accompanied by the creation of a centralized database of which the server is located on the territory of an ECHR Contracting Party. The geographical limitation to ECHR Contracting Parties allows us to review the envisaged cooperation in light of the jurisdictional and substantive guarantees provided by the ECHR, as notably developed by the European Court of Human Rights (ECtHR).

The authors have also taken into account the extensive legislation and case law of the European Union (EU) on data protection in order to develop an appropriate normative framework. The authors bear in mind that according to the Treaty on European Union (TEU), EU law does not govern national security matters as such.[8] Accordingly, from a formal perspective, it does not apply to the envisaged type of cooperation between intelligence and security services. Still, national security is not excluded from the scope of the Charter of Fundamental Rights of the European Union (the Charter),[9] including scrutiny by the European Court of Justice (ECJ), based on the Charter. At the very least, legal developments at the level of the EU may provide *guidance* for the cooperative arrangements with which we are concerned here. The strengthened cooperation between EU police services, accompanied by the

2 The CTG is not a formal EU institution, as the EU has no jurisdiction on national security matters. See art 4(2) Treaty on European Union. As no non-European states are involved, we will not discuss the participation and sharing of data by, and among, other states. See on US–EU data transfers notably: Mistale Taylor, 'Transatlantic Jurisdictional Conflicts in Data Protection Law: How the Fundamental Right to Data Protection Conditions the European Union's Exercise of Extraterritorial Jurisdiction' (PhD thesis, Utrecht University 2018).

3 See Review Committee on the Intelligence and Security Services (CTIVD), The multilateral exchange of data on (alleged) jihadists by the AIVD, Review report no 56, February 2018, 13 <https://english.ctivd.nl/documents/review-reports/2018/04/24/index> accessed 4 February 2019.

4 Compare the term 'participating state' as it is used in the context of the Organization for Security and Co-operation in Europe, which has no legal personality. See Conference on Security and Cooperation in Europe, Helsinki Final Act 1975.

5 CTIVD report no 56, above n 3, 13.

6 Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA (OJ L 135, 24.5.2016, 53–114).

7 Nico van Eijk and Cedric Ryngaert, 'Legal Basis for Multilateral Exchange of Information, Expert Opinion to the Review Committee on the Intelligence and Security Services' (CTIVD), appendix IV of CTIVD 2018 <https://english.ctivd.nl/documents/review-reports/2018/04/24/appendix-iv> accessed 4 February 2019. This report fed into CTIVD report no 56 (above note 3), which in turn informed a statement on 'Strengthening oversight of international data exchange between intelligence and security services', adopted in Bern on 22 October 2018 by the relevant services from the Netherlands, Belgium, Denmark, Norway, and Switzerland. The statement is available at <http://www.comiteri.be/images/pdf/publicaties/Common_Statement_EN.pdf> accessed 4 February 2019.

8 Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community: Treaty of Lisbon Treaty, art 4, para 2.

9 EU Charter of Fundamental Rights: Charter of Fundamental Rights of the European Union, OJ 2010 C 83/389.

creation of the aforementioned database managed by Europol (an EU agency), on the basis of an EU Regulation which provides for extensive data protection guarantees,[10] can be cited in this respect.

Methodologically, this article is based on currently applicable international law and ECHR/EU law, in particular with respect to questions of jurisdiction and liability, complemented by sector-specific insights from information and data protection law. This reflects the combined expertise of the authors.

The section 'Allocating responsibility' discusses the aspect of allocating responsibility on the basis of non-binding, information cooperation between intelligence and security services. The section 'Jurisdictional challenges' addresses the question whether individuals whose data are uploaded onto the database fall within the jurisdiction of any of the participating states. The section 'Responsibility in the context of data transfer' inquires what state's/states' responsibility is engaged for breaches relating to data transfer. Jurisdiction and responsibility issues are dealt with in the sections 'Jurisdictional challenges' and 'Responsibility in the context of data transfer'. The section 'Applicable data protection standards' examines what substantive data privacy protections apply in the context of the establishment of the database. Concluding observations are made in the section 'Conclusions'.

Allocating responsibility

Matters related to states' national security are sensitive. Accordingly, states are reluctant to share data regarding such matters, at least on the basis of formal legal regimes.[11] However, such reluctance need not extend to informal arrangements that are not legally binding, such as gentlemen's agreements or memoranda of understanding. Especially if they address transnational threats that are perceived to be very serious (eg terrorism, returning jihadists), political support for such international cooperation may well be forthcoming. Also in other fields of the law, states have entered into informal cooperative arrangements instead of adopting formal international legal instruments.[12]

It is apparent that national intelligence and security services wish to deepen cooperation regarding the exchange of data, including the establishment of databases, on the basis of informal cooperative arrangements.[13] This informal multilateral cooperation prompts the question how responsibility for data breaches[14] is precisely allocated: who bears obligations to guarantee an adequate level of data protection, and who is responsible in case of breach?

Under ECtHR law, ECHR Contracting Parties are not barred from pursuing international cooperation.[15] This includes exchange intelligence in the context of protecting national security.[16] Nonetheless, relevant ECtHR case law shows that states are precluded from setting up an international cooperative structure in such a way that individual rights are compromised.[17] In order to adequately protect human rights, the structure should provide for a level of protection that is at least equivalent to the level of protection normally offered by the ECHR.[18] This principle is known as the *Bosphorus* principle, based on the eponymous seminal decision of the ECtHR. Pursuant to *Bosphorus*, if an international arrangement or organization provides adequate guarantees, the participating states or member states which only implement obligations arising under the rules of the organization will not individually be held responsible. This principle does not apply when the state does

10 See above n 6.

11 It is then no surprise that EU law specifically excludes EU action regarding national security, as mentioned above. cf art 4, para 2 TEU.

12 See for a discussion: Pauwelyn, Wessel and Wouters (n 1).

13 See also Katarina Zivanovic, 'International Cooperation of Intelligence Agencies against Transnational Terrorist Targets' (2008) 8 (1) Connections 115–41; On accountability see: Hans Born, Ian Leigh and Aidan Wills, 'Making International Intelligence Cooperation Accountable' Printing Office of the Parliament of Norway, 2015, 105–88.

14 We use 'data breaches' as a generic indication for both personal data breaches (ie regulated in the EU General Data Protection Regulation (GDPR) and other data breaches, such as the theft of (confidential) government or business information. Given the international law and European human rights law perspective of this contribution, we only consider data breaches that rise to the level of violations of international or European (human rights) law.

15 *Bosphorus v Ireland* App no 45036/98 (ECtHR, 30 June 2005), para 152 (holding that the ECHR 'does not . . . prohibit Contracting Parties from transferring sovereign power to an international (including a supranational) organisation in order to pursue cooperation in certain fields of activity').

16 *Centrum För Rättvisa v Sweden* App no 35252/08 (ECtHR, 29 June 2018), para 150 (holding that 'it is evident that there must be a possibility of exchanging intelligence collected with international partners').

17 Above n 15, paras 15354. See also *Big Brother Watch And Others v The United Kingdom*, App nos 58170/13, 62322/14, and 24960/15 (ECtHR, 13 September 2018), para 424 ('[I]f Contracting States were to enjoy an unfettered discretion to request either the interception of communications or the conveyance of intercepted communications from non-Contracting States, they could easily circumvent their obligations under the Convention. Consequently, the circumstances in which intercept material can be requested from foreign intelligence services must also be set out in domestic law in order to avoid abuses of power').

18 Above n 15, para 155 ('State action taken in compliance with [legal obligations flowing from membership of an international organization] is justified as long as the relevant organization is considered to protect fundamental rights . . . in a manner which can be considered at least equivalent to that for which the Convention provides.'). Even if the provided protection is equivalent in general, in specific cases it should not be *manifestly deficient*. Ibid para 156.

more than just implement obligations, and exercises discretion.[19]

The *Bosphorus* principle was developed in the context of the transfer of powers to an intergovernmental organization (the EU). This is a separate international legal person, which may incur responsibility in its own right.[20] However, the Court's balancing of the valid aim of pursuing international cooperation with the countervailing imperative of providing adequate rights guarantees could extend to any type of international cooperation. This includes the informal type as envisaged by intelligence and security services, which does not task a separate legal person with managing a database.[21] If that is true, and the relevant gentlemen's agreement designates one or more state agencies as data controllers or processors, in particular the host state of the server, and moreover, if the agreement institutionalizes an adequate level of data protection, the host state, serving as a mere organ or agent of the international cooperative endeavour, could arguably invoke *Bosphorus* and limit its responsibility.

This applies only in the abstract, however. It may just happen that the cooperative arrangement itself does not provide for adequate data protection guarantees (behind which the host state could subsequently 'hide'), nor may it allocate responsibilities to the various actors involved. In the absence of a formal allocation of responsibility in a gentlemen's agreement and in the absence of specific provisions on data protection guarantees,[22] it will eventually be incumbent on the *host state itself* to provide adequate guarantees. This is very different from the typical *Bosphorus* scenario of a state being held responsible for implementing at the national level decisions taken by an international organization, or of a state being held responsible in respect of decisions of organs of an international organization: in the envisaged informal international cooperation between intelligence and security services, there is simply no separate international organization with the primary responsibility to guarantee rights.

In a situation of informal cooperation which does not establish a separate legal person, it appears instead that the participating states are *jointly responsible* for the processing of data and the management of the envisaged database, as they have a shared obligation to ensure an adequate level of data privacy (an obligation which otherwise would fall on the international organization). In case of data breaches, these states may *share responsibility* with each other. Shared obligations giving rise to possible shared responsibility is undertheorized in international law.[23] Still, there are some relevant precedents in international case law that indeed conceive of certain state obligations, namely to achieve a particular aim, as 'shared'. Notably *Certain Phosphate Lands*, a case before the International Court of Justice, can be cited. In this case, the Court ruled in a judgment on preliminary objections that Australia had obligations based on a trusteeship agreement regarding the territory of Nauru, an agreement to which also the UK and New Zealand were parties. As Australia was one of the three participating states, the Court held that it could consider a claim of a breach by Australia of the obligations arising under the agreement.[24] Somewhat similarly, the international arbitral tribunal in the *Eurotunnel* arbitration held that both France and the UK had joint obligations to maintain security and public order on the French side of the tunnel on the basis of a concession agreement with respect to the construction and operation of the Eurotunnel; in this case, this meant that a combined failure of both participating states led to a breach.[25] This arbitral award demonstrates that multiple states can have obligations with respect to a situation which is located on the territory of just one state. Also the jointly run database which is the object of our inquiry is, or will be located on the territory of one (host) state.

In the aforementioned cases, the very agreements between the participating states contained the relevant shared obligations. In contrast, informal agreements on cooperation between intelligence and security services may well remain silent on particular obligations,

19 *Matthews v UK* App no 24833/94 (ECtHR, 18 February 1999).

20 Cf Andrés Delgado Casteleiro, *The International Responsibility of the European Union: From Competence to Normative Control* (CUP 2016).

21 See Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA, and 2009/968/JHA. (OJ L 135, 24.5.2016, 53–114), which does designate such a person.

22 Ibid; Chapter V and Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016).

23 See however this important recent contribution the literature: Natasa Nedeski, 'Shared Obligations in International Law' (PhD thesis University of Amsterdam, 2017).

24 *Certain Phosphate Lands in Nauru (Nauru v Australia)* Preliminary Objections, Judgment, ICJ Reports 1992, 240 ('It cannot be denied that Australia had obligations under the Trusteeship Agreement, in its capacity as one of the three States forming the Administering Authority, and there is nothing in the character of that Agreement which debars the Court from considering a claim of a breach of those obligations by Australia.'). The case was eventually not pursued, however.

25 *The Channel Tunnel Group Ltd & France-Manche SA v United Kingdom & France*, Permanent Court of Arbitration (2007), Partial Award 2003-06 para 315.

notably regarding data protection. In this case, however, *existing* international obligations of the participating states will serve as constraints, in particular (for our purposes) international or regional human rights obligations pertaining to data protection. When pursuing international cooperation, participating states are arguably under a joint obligation to ensure the compatibility of the envisaged data processing with human rights protections. Obviously, a specification of the precise data protection guarantees in an international agreement furthers legal certainty,[26] but even without specification, the general principles of data protection remain applicable (see further the section 'Applicable data protection standards').

As argued, participating states may in principle share responsibility for breaches committed in the context of a shared database. However, the *host state*, ie the state on whose territory the server of the database is located, may have a heightened responsibility, in particular a specific duty of care. Precisely because of the territorial location of the server, or in any event the expectation of the initiators of the cooperative endeavour that the host state will develop and manage the database (which appears to be a common practice in security and intelligence circles), the host state can *in fact* exercise greater control and influence over the processing of data than other states can, and hence, it will also have a more extensive responsibility.[27] Regarding data privacy responsibility, this means that European judges are more likely to classify the intelligence and security services of the host state rather than the services of more remote participating states as data controllers or data processors which are bound by data privacy law.

The heightened responsibility of the host state does, however, not mean that the other participating states have no responsibility. Their responsibility, although possibly of a lesser variety, persists. As mentioned, this responsibility may be shared. In international law, it is not fully clear what consequences the establishment of shared responsibility entails, in particular regarding the obligation of cessation of the breaches, as well as the obligation to provide reparation for indivisible injury caused by these states' acts or omissions (ie injury that cannot be neatly divided and allocated to the various tortfeasors). With respect to the obligation to provide reparation, possibly the principle of joint and several responsibility, or liability as it is known in domestic law, could be applied.[28]

Jurisdictional challenges

In the section 'Allocating responsibility', it has been argued that pursuant to informal international cooperation arrangements between national intelligence and security services, participating states may in principle share responsibility for data breaches connected with the establishment of a joint database. However, under human rights treaties, such as the ECHR, before a state's responsibility can be engaged, it is required that the individuals affected by a data breach, fall *within the jurisdiction of that state*. This jurisdictional question is an important one, as it logically precedes the question of responsibility for breach, at least under the ECHR system: a state cannot breach an obligation which it does not owe in the first place. Inquiring into the issue of jurisdiction in a situation which has contact points with

26 Compare EU Regulation 2016/794 (Europol), which further defines the data protection guarantees regarding data transfer, control, and processing) or EU Directive 2016/680 (law enforcement).

27 In *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro)*, Judgment, ICJ Reports 2007 ICJ (2007), the International Court of Justice held Serbia responsible for its failure to prevent the genocide in Bosnia, in particular because Serbia was geographically close to the place of the events, and thus had a greater 'capacity to influence' the Bosnian Serbs, the actual perpetrators of the genocide. Cf ICJ, *Bosnia Herzegovina v Serbia and Montenegro* (2007), para 430 ('Various parameters operate when assessing whether a State has duly discharged the obligation concerned. The first, which varies greatly from one State to another, is clearly the capacity to influence effectively the action of persons likely to commit, or already committing, genocide. This capacity itself depends, among other things, on the geographical distance of the State concerned from the scene of the events, and on the strength of the political links, as well as links of all other kinds, between the authorities of that State and the main actors in the events.'). In some literature, the geographic approach to duties of care or due diligence duties has been criticized, and instead it has been proposed not to have the reach of human rights obligations be determined by territorial boundaries. Cf Mark Gibney, 'On Terminology' in Malcolm Langford and others (eds), *Global Justice, State Duties* (CUP 2013) 35. In our view, it has always to be ascertained whether the host state of the database, in light of the specific circumstances at hand, in comparison with other states, effectively has a greater capacity to secure the protection of personal data and to prevent breaches, eg because it places at the disposal of the cooperative endeavour certain infrastructure and own staff.

28 Cf John E Noyes and Brian D Smith, 'State Responsibility and the Principle of Joint and Several Liability' (1988) 13 Yale J Int'l L 225. The rationale of joint and several responsibility is that victims of breaches committed by multiple parties, who may be interrelated, should not be disadvantaged by the complicated legal relationships which these parties have *inter se*. Therefore, the victim may be allowed to invoke the responsibility for reparation of just one of the parties, for the entire injury produced by the parties' joint or concurrent action. The principle of joint and several responsibility is geared towards protecting the weaker party—which is allowed to target any participating state regarding the entire injury—and for that reason, may lend itself to application in the field of data protection law: the individual protected by data protection law can be considered as the weaker party *vis-à-vis* the overwhelming power of the state, and *a fortiori*, *vis-à-vis* the power of multiple cooperating states. See on joint and several liability in the field of data protection, eg art 82(4) GDPR ('Where more than one controller or processor, or both a controller and a processor, are involved in the same processing and where they are, under paragraphs 2 and 3, responsible for any damage caused by processing, each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject.').

multiple states comes down to determining the exact circle of states owing human rights obligations to an individual. Put differently, it is an investigation of the geographical or extraterritorial application of human rights law.[29] The relatively de-territorialized nature of transnational data exchange obviously complicates this investigation.[30]

The ECtHR has not yet specifically addressed the question if, and to what extent, data located in a joint database, or at least the individuals to whom the data relate, fall within a state's jurisdiction. However, clues as to the possible jurisdictional scope of the right to data protection can be found in existing ECtHR case law on the extraterritorial application of the ECHR. This case law puts forward 'control' as the relevant jurisdictional test: insofar as a state exercises control over an individual, the latter will fall within the former's jurisdiction. The ECtHR has interpreted the concept of control rather restrictively as control over (foreign) territory, or control on the basis of the exercise of 'public powers' abroad,[31] although some precedents use a personal control model (pursuant to which a state agent's control over an individual, regardless of location, serves as the jurisdictional trigger).[32]

It is emphasized that jurisdiction is not coterminous with responsibility under the ECHR system. A state's responsibility will only be engaged in case the state has committed an internationally wrongful act, ie a breach of an international obligation that can be attributed to the state.[33] Thus, a particular person may fall within a state's jurisdiction, but the state's responsibility may not be engaged because no wrongful act has been committed. *Vice versa*, a person may not fall within a state's jurisdiction—given the high threshold which applies for a finding of jurisdiction—but nevertheless be the victim of apparent breaches attributable to the state. This is so because under the secondary norms of the *lex generalis* of state responsibility, breach and attribution suffice for a finding of state responsibility, regardless of location,[34] whereas under the *lex specialis* of (some) primary international and regional human rights treaty law, in particular the ECHR, an additional jurisdictional requirement applies,[35] which is largely construed geographically. This differentiation may not seem to be entirely warranted, as it allows states to escape accountability for apparent breaches that are undeniably attributable to them.[36] Still, the differentiation flows from the very text of the ECHR as well as the case law of the ECtHR. Thus, it will also be applied in the analysis below.

In this section, it is ascertained to what extent persons affected by data breaches which occur *after the data has been transferred* to the database fall within the jurisdiction of the participating states eg as a result of poor data management and processing practices, design faults, or deliberate leaks. An analytical distinction is made between the host state, ie the participating state hosting the database on a server located on its territory, and the other participating states.

This section does not address the question whether the responsibility of the participating states could be engaged in respect of each other's acts. This is dealt with in the section 'Responsibility in the context of data transfer', which on the one hand examines whether (other) participating states, in particular the host state, could be responsible for data breaches committed by just one of them, and on the other hand whether states could be held individually responsible for transferring data to a deficient database managed by all states, although in particular by the host state.

Do persons whose data is stored in the database fall within the jurisdiction of the *host state*? Existing ECtHR

29 There is a large literature on the extraterritorial application of human rights, largely relating to military activities abroad. Cf Marko Milanovic, *Extraterritorial Application of Human Rights Treaties* (OUP 2011).

30 See for a discussion of data privacy extraterritoriality: Cedric Ryngaert (ed), 'Symposium Issue on Extraterritoriality and EU Data Protection' (2015) 5, 4 IDPL 221–25; Dan Jerker B Svantesson, *Solving the Internet Jurisdiction Puzzle* (OUP 2017). Note that Svantesson mainly theorizes prescriptive and adjudicatory jurisdiction, and addresses the question what state has *authority* to exercise jurisdiction over the Internet. *This* contribution, in contrast, focuses on *human rights* jurisdiction, and addresses the question under what circumstances states are under an *obligation* to apply human rights (privacy/right to data protection) 'extraterritorially'. This is a different inquiry.

31 *Al Skeini and others v United Kingdom* App no 55721/07 (ECtHR 7 July 2011).

32 See for a discussion and rationalization of relevant cases: S Miller, 'Revisiting Extraterritorial Jurisdiction: A Territorial Justification for Extraterritorial Jurisdiction under the European Convention' (2009) 20 (4) EJIL 1223–46.

33 Art 2 Draft articles on Responsibility of States for Internationally Wrongful Acts adopted by the International Law Commission at its 53rd session (2001) (ARSIWA). Acts and omissions of state organs, such as the intelligence and security services, can be attributed to the state pursuant to art 4 ARSIWA.

34 This means that a state's responsibility can be engaged with respect to breaches committed outside its territory.

35 Pursuant to the ECHR system, a state only has human rights obligations towards individuals, when the latter fall with the jurisdiction of the state (art 1 ECHR).

36 Vassilis P Tzevelekos, 'Reconstructing the Effective Control Criterion in Extraterritorial Human Rights Breaches: Direct attribution of Wrongfulness, Due Diligence, and Concurrent Responsibility' (2014) 36(1) Michigan J Int'l L 129. See, eg *Mothers of Srebrenica v The State of the Netherlands* (2014), case number C/09/295247 (District Court of The Hague), which attributed a large number of—potentially internationally wrongful – acts committed in the vicinity of Srebrenica to the Dutch state, but held that only limited number of these acts (or at least the persons affected by these acts) fell within the state's jurisdiction, thus engaging the responsibility of the state. See however *Mothers of Srebrenica v The State of the Netherlands* (2017), case number 200.158.313/01 (Court of Appeal The Hague), para. 38.7 (Court ruling that ECHR norms form part of the Dutch legal order, and that breaches of the ECHR are *ipso facto* breaches of the duty of care under Dutch civil law, apparently regardless of geographical location of the breaches).

case law shows that breaches of the right to privacy which occur *on a state's territory*, fall within that state's jurisdiction, regardless of the location (territorial or extraterritorial) of the persons to whom the data relate.[37] This would mean that breaches which relate to data stored on a server located on the territory of the host state, in principle fall within the latter's jurisdiction. Still, a decision of the UK Investigatory Powers Tribunal (2016) stated that 'a contracting state owes no obligation under Article 8 [ECHR, ie the right to privacy] to persons both of whom are situated outside its territory in respect of electronic communications between them which pass through that state'.[38] This could mean that states which establish and manage a joint database, including the host state, would have no obligations under Article 8 ECHR towards persons who are not present on their territory. Arguably, such a reading of the jurisdictional control standard applied by the ECtHR is too restrictive.[39] The UK Government appears to have realized this, as, in *Big Brother Watch* (2018), an application before the ECtHR in respect of the interception of external communications, it did not 'raise any objection under Article 1 of the Convention; nor did [it] suggest that the interception of communications ... was taking place outside the United Kingdom's territorial jurisdiction'.[40] The ECtHR therefore proceeded 'on the assumption that the matters complained of fall within the jurisdictional competence of the United Kingdom'.[41] An email, if one or both of the sender or recipient is overseas, is considered as an external communication,[42] which would thus fall within the intercepting state's jurisdiction.

It is recalled that, even if foreign persons whose data are processed in a central database fall within the jurisdiction of the host state, the latter could qualify or restrict its responsibility for possible breaches by transferring competences or sharing competences with other parties (see above the section 'Allocating responsibility'). In that case, the breaches continue to fall within the jurisdiction of the host state, but responsibility is shared with other states. As indicated above, however, the host state could have a heightened responsibility, a specific duty of care, in light of its proximity to the database and the server.

While it is likely that personal data found in the database, or at least persons to whom these relate, fall within the jurisdiction of the host state, it is less clear that they also fall within the jurisdiction of the other participating states, even if the responsibility for the database, and breaches committed during its operation, may in principle be shared (see the section 'Allocating responsibility'). Under the traditional territorial standard of jurisdiction, jurisdiction will not normally be found. However, the relevant test to determine jurisdiction may also be a functional one, based on control by state agents: insofar as a state agent performs acts with respect to data in the database, the state has a jurisdictionally relevant impact on the persons to whom the data relate.[43] The jurisdictional test then becomes one of 'virtual control': does the state have effective control over digital infrastructure, and hence an impact on the data and the persons to whom they relate?[44] It will depend on the exact operation of the database whether states other than the host state *in fact* exercise control. Insofar as the day-to-day management of the database has been left to the host state, it is unlikely that the relevant persons will fall within the jurisdiction of the other participating states.

Responsibility in the context of data transfer

In the section 'Allocating responsibility', it was argued that, in principle, data breaches occurring in the context of the management of the joint database could lead to

37 *Liberty v United Kingdom* App no 58243/00 (ECtHR, 1 July 2008) (Court implicitly acknowledges jurisdiction in a case of interception of data on the territory, even if the interception pertains to data of persons present outside the territory).

38 *Human Rights Watch Inc v The Secretary of State for the Foreign and Commonwealth Office*, [2016] UKIP Trib 15_165-CH [60].

39 See also Francesca Bignami and Giorgio Resta, 'Human Rights Extraterritoriality: The Right to Privacy and National Security Surveillance' in Eyal Benvenisti and Georg Nolte (eds), *Community Interests Across International Law* (OUP 2017) 374–78.

40 *Big Brother Watch* (n 17). We note that the case was decided by one of the chambers of the court and still might be heard by the Grand Chamber after this article was finished.

41 Ibid. See also Marko Milanovic, 'ECtHR Judgment in Big Brother Watch v UK' (*EJIL:Talk!*, 17 September 2018), <https://www.ejiltalk.org/ecthr-judgment-in-big-brother-watch-v-uk/> ('The Court could easily have examined the question proprio motu because it concerns the very applicability of the Convention, but (again, wisely) chose not to.').

42 See evidence given to the Intelligence and Security Committee of Parliament in October 2014 by the Secretary of State for the Foreign and Commonwealth, cited in *Big Brother Watch*, para 71 (above (n 17)).

43 Marko Milanovic, 'Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age' (2015) 56 (1) Harv Int'l L J 126 ('I do not see why the ECHR would not apply to a similar search of my laptop by U.K. agents operating in Serbia, whether lawfully or unlawfully. In other words, the location of both the individual and the interference seems to be irrelevant under the logic of the personal model.').

44 Bignami and Resta (n 39) 375–76; Peter Margulies, 'Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility' (2013) 14 Melb J Int'l L 496, 514–15; Valsamis Mitsilegas, 'Surveillance and Digital Privacy in the Transatlantic "War on Terror." The Case for a Global Privacy Regime' (2016) 47(3) Columbia Human Rights L Rev 1–77; submission of the International Commission of Jurists to the ECtHR, cited in *Big Brother Watch*, para 299 ('the fact that, in a mass surveillance operation, elements of the interference with rights might take place outside a State's territorial jurisdiction didn't preclude that State's responsibility, since its control over the information was sufficient to establish jurisdiction').

shared responsibility of the participating states, although it was emphasized that the host state may have a heightened responsibility. In the section 'Jurisdictional challenges', it was set out that persons affected by data breaches linked to the database do nevertheless not, as a matter of course, fall within the human rights jurisdiction of the participating states (including even the host state). Still, depending on the jurisdictional model used, and how it is interpreted, relevant persons may well fall within the jurisdiction of the host state, and to a lesser extent of other participating states.

This section focuses on the somewhat distinct issue of *data transfer*. It is ascertained what obligations the participating states, or least those responsible for managing the database have in respect of data received from individual states, and *vice versa*, what obligations individual states have in respect of data transferred to the database. The sub-section 'Participating states' responsibility for data breaches' seeks to answer the question whether the participating states in general, although more specifically the host state, are/is responsible for data breaches committed by just one state, which uploads the 'contaminated' data onto the database (assuming that no separate breaches subsequently occur). The sub-section 'Participating states' individual responsibility for database deficiencies' studies the reverse scenario and examines whether a participating state is individually responsible for transferring data to a deficient international database, ie a database which does not provide adequate data protection guarantees.

Participating states' responsibility for data breaches

So far, we have addressed breaches which occur after the transfer. Breaches could however also take place *before* transfer: the participating state may itself commit a breach, and subsequently upload the 'contaminated' data onto the database. The question arises whether the persons to whom the data relate are within the jurisdiction of the other participating states, in particular of the host state.[45] Translated into responsibility terms, the question is whether participating states' responsibility is engaged for the deficient quality of the data supplied by one participating state.

From a jurisdictional perspective, it can be submitted that the relevant persons do in principle not fall within the jurisdiction of the participating states other than the state transferring the contaminated data, at least not under the dominant spatial model of jurisdiction.[46] After all, the other participating states did not control the collection of the contaminated data. Under a more progressive personal model of jurisdiction, which would consider the normative or factual relationship of a participating state with a person, eg the transfer of data related to him on the basis of an international agreement, jurisdiction may possibly be found, but it is hardly certain whether the ECtHR would go down this path.

Even if jurisdiction were to be found, however, it is not certain whether the responsibility of the participating states, and in particular of the host state, will automatically be engaged.

The law of responsibility does not as such recognize the complicity-after-the-fact scenario with which we are concerned here.[47] Thus, in *Big Brother Watch* (2018), the ECtHR did not consider the law of state responsibility relevant to determine ECHR compliance of an intelligence sharing regime (in the case between the US and the UK), on the ground that 'the interference under consideration in this case does not lie in the interception itself, which did not, in any event, occur within the United Kingdom's jurisdiction, and was not attributable to that State under international law'.[48]

Nevertheless, the responsibility of a state, eg the host state, may be engaged for knowingly uploading contaminated data, an issue that was *not* addressed by the ECtHR in *Big Brother* Watch.[49] Thereby, it may facilitate and entrench breaches committed by other states in

45 It is assumed here that these persons are within the jurisdiction of the state committing the breach, although even that is not fully clear.

46 That being said, a progressive, broadly conceived personal model of jurisdiction may leave some room for an affirmative answer. See above (n 43) 123–24 ('A more difficult problem arises if a state engages in surveillance of its own population and then provides the information it collected to a third party. The "Five Eyes" states share signals intelligence and the data they collect with one another, although the specifics are of course unclear. The individuals concerned could be within the jurisdiction of the collecting/ sending state, but not necessarily under the jurisdiction of the receiving state, at least not under the spatial model.') (footnote omitted)

47 ILC Commentary (1) to art 16 ARSIWA, *Yearbook of the International Law Commission, 2001*, vol II, Part Two, 66; Helmut Philipp Aust, *Complicity and the Law of State Responsibility* (CUP 2011) 222.

48 *Big Brother Watch*, para 420 (see above (n 17)), adding in the same paragraph that '[a]s the communications are being intercepted by foreign intelligence agencies, their interception could only engage the responsibility of the respondent State if it was exercising authority or control over those agencies', and that '[e]ven when the United Kingdom authorities request the interception of communications (rather than simply the conveyance of the product of intercept), the interception would appear to take place under the full control of the foreign intelligence agencies'.

49 The Court only reviewed the 'subsequent storage, examination and use by the intelligence services of the respondent State' in light of the general guarantees regarding the acquisition of surveillance material, as they have been set out in the *Zakharov* case'). Ibid paras 421–22. The Court does not address the effects of data or evidence which the foreign state has acquired in an unlawful manner, eg through torture.

violation of the duty of non-recognition.[50] International law, however, limits such responsibility to serious breaches of peremptory norms, such as the prohibition of genocide.[51] Data protection breaches do not rise to the level of such breaches. Still, the International Court of Justice has implied that also breaches of *erga omnes* obligations could trigger the duty of non-recognition and the prohibition for third states to assist in the maintenance of a situation created by such breaches.[52] *Erga omnes* obligations are obligations in which the entire international community has an interest. It could be argued that data protection obligations are such obligations, but even then, for the aforementioned duty to be triggered, the breach has to be serious.[53] This creates a particularly high threshold, which may be unlikely to be met.

From a practical perspective, if states' responsibility could be engaged on these grounds, they have to put in place control systems that prevent contaminated data from being uploaded onto the system, or at least from being subject to further processing and dissemination to other services. Particular obligations rest on the host state of the database. In any event, purely from a territorial jurisdiction perspective, as the ECtHR pointed out in *Big Brother Watch*, a receiving state may be interfering in the right to privacy as soon as it receives intercepted material, and subsequently stores, examines and uses it.[54] As the ECtHR held in this respect: 'if Contracting States were to enjoy an unfettered discretion to request either the interception of communications or the conveyance of intercepted communications from non-Contracting States, they could easily circumvent their obligations under the Convention'.[55]

Participating states' individual responsibility for database deficiencies

The sub-section 'Participating states' responsibility for data breaches' addressed the responsibility of 'the system' in connection with breaches committed by one participating state. This section addresses the reverse scenario of the responsibility of one state in connection with breaches committed by 'the system'. More specifically, it examines a state's individual responsibility for transferring data to an international database which does not provide adequate data protection guarantees.

It may appear that, when a state has transferred (non-contaminated) data to an international database (largely) managed by the host state, the former does not bear responsibility for subsequent breaches committed by the latter. After all, the former does no longer control the data after the transfer (unless of course, it were to be involved in the management of the database, as highlighted in the section 'Allocating responsibility'). The ECtHR has not addressed this question in the specific context of data protection. However, it has addressed a similar question in the extradition and deportation context. It held that the responsibility of a Contracting Party is engaged in case it extradites or deports an individual to another state, including a non-Contracting Party, where it is foreseeable that he will be exposed to a (serious) ECHR violation.[56] Under this risk-based responsibility standard, extraditions and deportations were deemed impermissible under the ECHR if the state of destination might impose the death penalty or life without parole, where torture, or inhuman or degrading treatment are routine practices, or where manifest violations of the right to a fair trial may occur, were deemed impermissible under the ECHR.[57] *Mutatis mutandis*, in the field of data protection, arguably a state's responsibility under the ECHR is engaged when it is foreseeable that the international database to which it transfers data is deficient from a data protection perspective. Under the general law of state responsibility (as opposed to ECHR law), however, it is less clear whether in such a situation, responsibility would be attributed to the transferring state, although an argument in favor of responsibility can certainly be made.[58]

50 Art 41(2) ARSIWA. See on facilitation with respect to data exchange, from a public international law perspective, albeit in the specific context of providing data and granting a third party state access to communication systems, also Anne Peters, 'Privacy, Rechtsstaatlichkeit, and the Legal Limits on Extraterritorial Surveillance' in Russel A Miller (ed), *Privacy and Power: A Transatlantic Dialogue in the Shadow of the NSA-Affair* (Washington and Lee University 2017) 170 (arguing that states should 'refrain from collaborating with a third state and assisting that state's violations of privacy through surveillance measures').

51 Art 41(2) in conjunction with art 40 ARSIWA.

52 *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion*, ICJ Reports 2004, 136 ICJ (2004), paras 154–55.

53 The same rules govern the bilateral issue of one state's responsibility for data breaches committed by another state: under the law of responsibility, the former's responsibility can be engaged if it consciously accepts data knowing that they were collected by means of a serious breach by another state, and in this manner recognizes or encourages that breach.

54 *Big Brother Watch* (see above (n 17)) para 421.

55 Ibid para 424.

56 *Soering v United Kingdom* App no 14038/88 (ECtHR, 25 January 1989).

57 *Harkins and Edwards v United Kingdom* App nos 9146/07 and 32650/07, (ECtHR, 12 January 2012). See also a similar kind of decision by the ECJ: ECJ, *MP v Secretary of State for the Home Department* case no C-353/16 (ECJ, 24 April 2018).

58 Art 16 ARSIWA provides as follows: 'A State which aids or assists another State in the commission of an internationally wrongful act by the latter is internationally responsible for doing so if:
(a) That State does so with knowledge of the circumstances of the internationally wrongful act; and
(b) The act would be internationally wrongful if committed by that State.' For responsibility to be attributed on the basis of this provision,

If the transferring state's responsibility could be engaged on the basis of exposure to breach, or facilitation, to avert such responsibility it is incumbent on that state to seek guarantees from 'the system' that no data breaches will occur after transfer.[59] In this respect, mention could be made of the EU's practice of seeking guarantees concerning adequate data protection from third states to which data are transferred, and the strict supervision exercised by European courts in this respect.[60] In case the given guarantees are *a priori* satisfactory in light of the circumstances and the information available at the moment of transfer, the transferring state cannot be held responsible for breaches committed by 'the system'. After all, the responsibility at issue is based on due diligence; it is not objective.

The analysis in this the sub-section 'Participating states' individual responsibility for database deficiencies' applies to *any* state transferring data to 'the system'. This includes fully participating states, but also other states which, on the basis of an informal agreement with the participating states, are allowed to upload (some) data onto the system. It bears emphasis, however, that the responsibility of the participating states in connection with breaches committed at the level of the system may also be more directly engaged on the basis of the attribution of systemic conduct. As described in the section 'Allocating responsibility', the participating states themselves have set up the database; in the absence of a separate international legal person managing the database, all of them may incur shared responsibility for systemic failures. At the same time, however, it has been signalled that, in light of how the database will be managed in practice, responsibility may rest mainly with the host state. This means that there may be a non-negligible residual role for the sort of transfer-related, risk-based responsibility of the other participating states, as discussed in this section.

Applicable data protection standards

Assuming that states are indeed responsible for (breaches occurring in relation to) the establishment of a database, a final issue pertains to the applicable standards governing the protection of data transferred to and stored on that database. As data transfer to, and management of the database involves a large number of states, it is arguable that applicable standards should not be drawn from one specific jurisdiction. Instead, they should be based on general principles of data protection law, either directly or via incorporation in national law.

The general framework for data protection law is laid down in Article 8 ECHR, in Convention 108 of the Council of Europe,[61] and in Articles 7 and 8 EU Charter on Fundamental Rights.[62] Sector-specific instruments such as the General Data Protection Regulation (2016/679), the Directive on the protection of personal data being processed in the context of law enforcement and judicial activities (2016/680) or the Europol Regulation (2016/794) do not apply to the activities of national security services, as, *per* Article 4(2) TEU, EU law does not apply to national security.

The general provisions in respect of data protection in Article 8 ECHR and Articles 7 and 8 Charter have been

actual knowledge on the part of the assisting state (in our case the state transferring the data) is required. Cf International Law Commission, Commentary Draft articles of Responsibility of States for Internationally Wrongful Acts, UN Doc A/56/10 (2001), 66. Constructive knowledge does not suffice. It is not clear, however, whether the knowledge standard set out in art 16 ARSIWA represents customary international law. In some literature, in any event, it has been argued that a state's acts of assistance to another state may fall within the jurisdiction of the former, and may engage its responsibility, in case it is foreseeable that a human rights violation will take place in the other state. M Jackson, 'Freeing Soering: The ECHR, State Complicity in Torture, and Jurisdiction' (2016) 27(3) EJIL 817.

59 Compare the practice of diplomatic assurances in extradition law. Cf AD Jillions, 'When a Gamekeeper turns Poacher: Torture, Diplomatic Assurances and the Politics of Trust' (2015) 91(3) International Affairs 489.

60 Case C-362/14, *Maximillian Schrems v Data Protection Commissioner*, judgment of 6 October 2015 (Grand Chamber) (ECLI:EU:C:2015:650) para 106; Commission Implementing Decision of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU–US Privacy Shield, Brussels (COM 2016) 4176 final; Art 45(1) GDPR ('A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection.').

61 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28 January 1981, <www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108>. A modernized version of the convention—called Convention 108+—has been adopted in May 2018 and opened for signature and ratification (<https://www.coe.int/en/web/data-protection/convention108/modernised>). The Convention has been instrumental in the European Court of Human Rights' recognition of privacy/data protection. See Council of Europe, Convention 108+ Convention for the protection of individuals with regard to the processing of personal data, explanatory report, with references to relevant ECtHR case law. See, egp 26 of the report on the exceptions that are allowed in respect of processing activities for national security and defence purposes, and the applicable requirements in relation to the independence and effectiveness of review and supervision mechanisms (citing *inter Roman Zakharov v Russia* App no 47143/06 (ECtHR, 4 December 2015); *Szabó and Vissy v Hungary*, App no 37138/14 (ECtHR, 12 January 2016).

62 Arts 7 and 8 of the EU Charter on Fundamental Rights. The relationship between the ECHR and the Charter is provided for in art 52, para 3, of the Charter, which provides as follows: 'In so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection.'

applied and developed in extensive case law of the ECtHR and the ECJ. Although a detailed discussion of this case law falls outside the scope of this article, some of the landmark cases can be mentioned. In the context of the ECHR, the ECtHR has summarized and partly renewed its views on secret surveillance in the *Zakharov* case, followed by the *Szabó and Vissy* case and the *Big Brother Watch* case.[63] Relevant ECJ cases include *Digital Rights Ireland*, *Schrems*, *Tele2/Watson* and *PNR-Canada*, which pertain to the tension between fundamental rights and national security, including in an extra-EU context.[64] These cases also make clear that the ECJ claims certain authority over national security based on the Charter, and does not seem to see its authority limited by the national security exception contained in Article 4, paragraph 2 of the TEU.[65] The relevance of this provision—which states that national security remains the sole responsibility of each Member State—is a central element in the pending UK case of *Privacy International v Secretary of State*.[66] The ECJ is asked whether, having regard to Article 4 TEU and Article 1(3) of Directive 2002/58/EC4 on privacy and electronic communications (the 'e-Privacy Directive'), a requirement set by the Secretary of State to a provider of an electronic communications network that it must provide bulk communications data to the Security and Intelligence Agencies (SIAs) of a Member State falls within the scope of Union law and of the e-Privacy Directive.[67]

From the case law, general principles of data protection law can be derived which remain relevant in the context of national security, and consequently also for multilateral data exchanges. These principles, which usually correspond with what is known as 'Fair Information Practices' (FIPs, as developed within the framework of the Organization for Economic Cooperation and Development),[68] include for example (1) data processing must be linked to a specific purpose and not go further than necessary (purpose limitation and data minimisation); (2) the quality and security of the data must be safeguarded; (3) rights of data subjects must be observed; (4) functional approach (eg where it concerns the responsibilities for the responsible party as well as the processer); (5) necessity/proportionality, also aimed at elements such as retention periods, the nature of the data (more or less sensitive), subsidiarity, and the use of methods that are 'state-of-the-art'. Furthermore, jurisprudence attaches high value to an adequate system of oversight.[69]

In the recent *Big Brother Watch* case, the ECtHR essentially (re)confirms these principles in a national security context, mentioning the following six requirements: (a) the nature of offences which may give rise to an interception order; (b) a definition of the categories of people liable to have their communications intercepted; (c) a limit on the duration of interception; (d) the procedure to be followed for examining, using and storing the data obtained; (e) the precautions to be taken when communicating the data to other parties; (f) and the circumstances in which intercepted data may or must be erased or destroyed. As to the aspect of oversight the court restates the need for 'arrangements for supervising the implementation of secret surveillance measures, any notification mechanisms and the remedies provided for by national law'.[70] It is important to note that these criteria stem from an earlier decision on criminal investigations.

As stated before, although the various sector-specific data protection instruments do not apply directly to national security matters, they represent the aforementioned principles at a more detailed level. This is most visible at the EU level, where in recent years not only the GDPR was adopted, but also two instruments related to law-enforcement (Europol Regulation and Police Enforcement Directive).[71] In many respects, these three instruments are alike. Duties of care and provisions on security and privacy by design/default are often

63 *Roman Zakharov v Russia* App no 47143/06 (ECtHR, 4 December 2015); *Szabó and Vissy v Hungary*, App no 37138/14 (ECtHR, 12 January 2016) and *Big Brother Watch* (see above (n 17)).

64 Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* ('Digital Rights Ireland'), judgment of 8 April 2014, ECLI:EU:C:2014:238; Case C-362/14, *Maximillian Schrems v Data Protection Commissioner*, judgment of 6 October 2015 (Grand Chamber) (ECLI:EU:C:2015:650); Joined Cases C-203/15 and C-698/15, *Tele2 Sverige AB v Post-och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others* ('Tele2/Watson'), judgment of 21 December 2016, ECLI:EU:C:2016:970; Opinion procedure 1/15, *Draft agreement between Canada and the European Union — Transfer of Passenger Name Record data from the European Union to Canada* ('PNR-Canada'), opinion of 26 July 2017, ECLI:EU:C:2017:592.

65 'The Union shall respect the equality of Member States before the Treaties as well as their national identities, inherent in their fundamental structures, political and constitutional, inclusive of regional and local self-government. It shall respect their essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. In particular, national security remains the sole responsibility of each Member State.'

66 *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others*, C-623/17.

67 See on bulk collection also Fred H Cate and James X Dempsey (eds), *Bulk Collection. Systematic Government Access to Private-Sector Data* (OUP 2017).

68 Cf OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (2013). See also: Christopher Kuner, *Transborder Data Flow Regulation and Data Privacy Law* (OUP 2013).

69 Cf *Roman Zakharov v Russia* App no 47143/06 (ECtHR, 4 December 2015), para 238.

70 *Big Brother Watch*, above (n 17) para 307.

71 See above nn 21–22.

similarly phrased. Duties only divert for sector-specific reasons, such as when and how to inform a citizen versus a suspect. One can assume that regarding data protection, national security regulation will increasingly be measured by what is considered as relevant both in general and in the context of law-enforcement. The reasoning of the ECtHR in *Big Brother Watch*—applying criminal investigations criteria to national security—is a clear illustration of such an approach.

This development directly impacts the joint database that is the object of our research. When the participants are EU Member States or European Free Trade Association (EFTA) members with aligned legislation, it is likely that in case of judicial review, courts will apply a very strict 'adequacy test' or will just apply norms directly taken from existing (EU) regulatory frameworks. Such an approach would also be compliant with the ECtHR framework (as was again demonstrated in *Big Brother Watch*), which belongs to the EU *acquis*: for reasons of national security, privacy may be interfered with, but an interference always needs to be necessary in a democratic society. This puts a serious burden of proof on member states, which will have to argue why rules on procession of data or oversight should be different in national security cases.

Clear examples on the potential impact can be derived from the *Digital Rights Ireland* case,[72] where the ECJ annulled an EU Directive on data retention for various reasons including insufficient limitations on the duration of the data retention, thereby illustrating the impact of the principle of data minimization. A joint database cannot exempt the hosting state from taking responsibility in this respect independently from the national rules that govern the contribution of a participating state. Hosting information in the database not meeting the requirements set by the ECJ would result in a breach that needs to be remedied.

As mentioned, data protection/national security laws as well as case law place special emphasis on independent oversight and transparency. Data processing in the context of national security without oversight and effective remedies is not compatible with fundamental rights frameworks.[73] While ECtHR case law has independently developed the need for oversight, the EU Charter explicitly prescribes independent oversight in respect of data protection in Article 8, paragraph 3. Multilateral information exchange must therefore comply with the same principles of oversight. With due regard for the existing sector-specific applications, it is reasonable to assume that oversight responsibilities in respect of the sort of multilateral cooperation contemplated by intelligence agencies, must be along the same lines in order to pass judicial review. Not having a system of sufficient oversight in place could constitute breach of the governing principles and be challenged in court. It is of note that, *per* case law of the ECtHR, proper supervisory elements may even counterbalance regulatory shortcomings in the context of data communication to other states or international organizations.[74]

In the specific case of a joint database hosted in the Netherlands under the direct control of the Dutch government, we assume full applicability of Dutch law.[75] Acts of the government must, at a minimum, comply with national law and can be challenged in court. Similar to the European situation, in the Netherlands, national security is not part of the ordinary legal framework regarding privacy protection, nor is it part of the instruments applicable to law-enforcement. A special act, the Intelligence and Security Services Act 2017, lays down rules for data collection and data processing by the intelligence and security services.[76] This act does not contain specific provisions on a joint database. However, in a report, the Dutch Review Committee on the Intelligence and Security Services (CTIVD) has made it clear that activities relating to the joint database do fall within its supervisory authority.[77] The CTIVD therefore has the authority on issues like compliance with national (as well as European and international) principles on issues such as data retention.[78]

72 See above n 64.

73 Sarah Eskens, Ot van Daalen and Nico van Eijk, '10 Standards for Oversight and Transparency of National Intelligence Services' (2016) 8(3) JNSLP 553; *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU - Volume II: field perspectives and legal update*, European Union Agency for Fundamental Rights (FRA), Vienna, 2017; Thorsten Wetzling and Kilian Vieth, *Upping the Ante on Bulk Surveillance An International Compendium of Good Legal Safeguards and Oversight Innovations*, Heinrich Böll Foundation, Publication Series on Democracy, volume 50, Berlin, 2018.

74 See n 16, para 151.

75 The AIVD, the Dutch General Intelligence and Security Service, is part of the Ministry of the Interior and Kingdom Relations (BZK). Therefore, it falls under full ministerial responsibility.

76 Wet van 26 juli 2017, houdende regels met betrekking tot de inlichtingen- en veiligheidsdiensten alsmede wijziging van enkele wetten (Wet op de inlichtingen- en veiligheidsdiensten 2017 / Intelligence and Security Services Act), Stb. (Official Journal, the Netherlands) 2017, 317.

77 Review Committee on the Intelligence and Security Services (CTIVD), The multilateral exchange of data on (alleged) jihadists by the AIVD, Review report no 56, February 2018, <https://english.ctivd.nl/documents/review-reports/2018/04/24/index>.

78 The CTIVD can only report and does not offer remedies on its own. While going beyond the scope of this contribution, whether or not the Dutch system offers a system of *oversight* that meets the standards of European courts requires further attention.

Conclusions

Increasing multinational cooperation between intelligence and security services, including the establishment of a joint database on (alleged) jihadists, raises legal concerns over the protection of personal data, in particular with respect to the allocation of responsibility among participating states, the geographic scope of fundamental data protection norms, and the applicable law. In this contribution, it has been argued that states participating in multinational cooperative efforts may share responsibility, eg in relation to a shared database, but that, for reasons of proximity, the host state of the server has heightened duties of care. It has also been argued that where a participating state, in particular the host state, exercises virtual control (jurisdiction) over an individual person's data, such a state has data protection obligations towards that person, regardless of the latter's location. Participating states, and, as stated before, in particular the host state, are under an obligation to put in place adequate control systems, including with a view to preventing the transfer of data that have been gathered by state in breach of data protection guarantees. If systemic failures in the multilateral system are identified, states are barred from transferring data to the system, unless they can obtain credible guarantees that data will be adequately protected. General principles of data protection law, derived from case law as well as general or sector-specific regulations, govern the processing and transfer of data in the context of multinational intelligence cooperation, including the management of a joint database. There is no reason not to apply them in the context of national security.

doi:10.1093/idpl/ipz001