ECLI:NL:RBDHA:2015:2498

Court of The Hague
Date of Ruling : 11 March 2015
Case Number: C/09/480009 / KG ZA 14/1575
Find the original Dutch version here.

Ruling

District Court of The Hague

Verdict in preliminary relief proceedings dated 11 March 2015

In the case of

1. The foundation
   Stichting Privacy First
2. The association
   Nederlands Juristen Comité voor de Mensenrechten
3. the association
   Nederlandse Vereniging van Strafrechtadvocaten
4. the association
   Nederlandse vereniging van Journalisten
5. the limited liability company
   BIT B.V.
6. the limited liability company
   SpeakUP B.V.
7. the limited liability company
   VOYS B.V.
   claimant
   lawyer: mr. F.F. Blokhuis of Amsterdam

against:

The Kingdom of the Netherlands
repondent
Lawyer: mr. R.J.M. van den Tweel of The Hague

Parties are from hereon out referred to as 'Privacy First cs' and 'the State' respectively.

1 The Facts

Based on the documents and the hearing held on 18 February 2015 the facts are as follows.

1.1. Privacy First cs are organizations that have as their goal to protect human rights, including the right to privacy (plaintiffs sub 1 and 2), associations of professional groups with a right to confidentiality (plaintiffs sub 3 and 4) and providers of telecommunication services and public telecommunication networks (plaintiffs sub 5,6 and 7).

1.2. On 15 March 2006 the Directive 2006/24/EG has been published in the Official Journal of the European Union, on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (hereinafter: Data Retention Directive). The Data Retention Directive entered into force twenty days after that.

1.3. Among other things the Data Retention Directive states:

> *"Article 1.*
> ***Subject matter and scope***
>
> *1. This Directive aims to harmonise Member States' provisions concerning the obligations of the providers of publicly available electronic communications services or of public communications networks with respect to the retention of certain data which are generated or processaed by them, in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law.*
> *2. This Directive shall apply to traffic and location data on both legal entities and natural persons and to the related data nec- essary to identify the subscriber or registered user. It shall not apply to the content of electronic communications, including information consulted using an electronic communications network. "*

1.4. Implementation of the Data Retention Directive in Dutch legislation has led to the Act of 18 July 2009 on amending the Telecommunication Act and the Act on Economic Crimes in connection with the offering of public electronic communication services and amending Directive 2002/58/EG (Act Data Retention Telecommunication Services, to be found in: Stb. 2009, 333, from hereon out: the Wbt). The Wbt entered into force on 1 September 2009. Among other things the Wbt states:

> *"**ARTICLE 1***
>
> *The Telecommunication Act is amended as follows:*
> *(…)*
> *Article 13.2a will state:*
>
> ***Article 13.2a***
>
> 1. *In this article the following definitions will apply:*
>   a. *'data' means traffic data and location data, (…) and the related data necessary to identify the subscriber or user;*
>   b. *'unsuccessful call attempt' means a communication where a telephone call has been successfully connected but not answered or there has been a network management intervention.*
> 2. *Those that offer public telecommunication networks or public telecommunication services retain the indicated data that are defined in an attachment to this act, to the extent that those data are generated or processed in the framework of, for the purpose of the investigation, detection and prosecution of serious crime.*

3. *The data, as referred to in the second paragraph, are retained by the providers for a period of twelve months, starting from the date of the communication.*
4. *The obligation, as referred to in the second paragraph, concern data of unsuccessful call attempts, insofar as these data are generated, processed and saved or logged by the providers of publicly available electronic communications services or of a public communications network. "*

1.5. By Act of 6 July 2011 article 13.2a, third paragraph, of the Telecommunication Act was amended again. That paragraph has since then held (Stb. 2011, 350):

> *"3. The data, as referred to in the second paragraph, are retained by the providers for a period of:*
>
> *a. twelve months for data in connection with telephony on a landline or mobile network (…), or*
>
> *b. six months for data in connection with internet access, e-mail by internet and internet telephony, (…) starting from the date of the communication."*

1.6. The Court of Justice of the European Union (hereinafter: the Court) has invalidated on 8 April 2014, with retroactive effect, the Data Retention Directive (Court of Justice EU 8 April 2014, in Joined Cases C‑293/12 and C‑594/12, Digital Rights Ireland Ltd and Seitlinger and others.) In its judgment the Court has tested the validity of the Data Retention Directive against articles 7 and 8 of the Charter of fundamental Rights of the European Union (hereinafter: the Charter). According to the Court, the Data Retention Directive constitutes a very wide and especially serious breach of the protected rights of article 7 and 8 of the Charter. The Courts further considered that the Data Retention Directive's material scope is to combat serious crime and thus ultimately contribute to public safety and that the prescribed retention of data actually responds to a public interest goal. The Court has ruled that the legislator of the European Union crossed the boundaries of the proportionality principle that it has to take into account in light of articles 7, 8 and 52, paragraph 1, of the Charter. In the judgment the following is mentioned, in the Dutch translation, [Here I will adhere to the English language versions, AB]:

> "*49. As regards the question of whether the retention of data is appropriate for attaining the objective pursued by Directive 2006/24, it must be held that, having regard to the growing importance of means of electronic communication, data which must be retained pursuant to that directive allow the national authorities which are competent for criminal prosecutions to have additional opportunities to shed light on serious crime and, in this respect, they are therefore a valuable tool for criminal investigations. Consequently, the retention of such data may be considered to be appropriate for attaining the objective pursued by that directive.*
>
> *(…)*
>
> *51 As regards the necessity for the retention of data required by Directive 2006/24, it must be held that the fight against serious crime, in particular against organised crime and terrorism, is indeed of the utmost importance in order to ensure public security and its effectiveness may depend to a great extent on the use of modern investigation techniques.*

However, such an objective of general interest, however fundamental it may be, does not, in itself, justify a retention measure such as that established by Directive 2006/24 being considered to be necessary for the purpose of that fight.

52 So far as concerns the right to respect for private life, the protection of that fundamental right requires, according to the Court's settled case-law, in any event, that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary (Case C‑473/12 IPI EU:C:2013:715, paragraph 39 and the case-law cited).

(…)

54 Consequently, the EU legislation in question must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards so that the persons whose data have been retained have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access and use of that data (see, by analogy, as regards Article 8 of the ECHR, Eur. Court H.R., Liberty and Others v. the United Kingdom, 1 July 2008, no. 58243/00, § 62 and 63; Rotaru v. Romania, § 57 to 59, and S. and Marper v. the United Kingdom, § 99).

55 The need for such safeguards is all the greater where, as laid down in Directive 2006/24, personal data are subjected to automatic processing and where there is a significant risk of unlawful access to those data (see, by analogy, as regards Article 8 of the ECHR, S. and Marper v. the United Kingdom, § 103, and M. K. v. France, 18 April 2013, no. 19522/09, § 35).

56 As for the question of whether the interference caused by Directive 2006/24 is limited to what is strictly necessary, it should be observed that, in accordance with Article 3 read in conjunction with Article 5(1) of that directive, the directive requires the retention of all traffic data concerning fixed telephony, mobile telephony, Internet access, Internet e-mail and Internet telephony. It therefore applies to all means of electronic communication, the use of which is very widespread and of growing importance in people's everyday lives. Furthermore, in accordance with Article 3 of Directive 2006/24, the directive covers all subscribers and registered users. It therefore entails an interference with the fundamental rights of practically the entire European population.

57 In this respect, it must be noted, first, that Directive 2006/24 covers, in a generalised manner, all persons and all means of electronic communication as well as all traffic data without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime.

58 Directive 2006/24 affects, in a comprehensive manner, all persons using electronic communications services, but without the persons whose data are retained being, even indirectly, in a situation which is liable to give rise to criminal prosecutions. It therefore 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. Furthermore, it does not provide for any exception, with the result that it

applies even to persons whose communications are subject, according to rules of national law, to the obligation of professional secrecy.

59 Moreover, whilst 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.

60 Secondly, not only is there a general absence of limits in Directive 2006/24 but Directive 2006/24 also fails to lay down any objective criterion by which to determine the limits of the access of the competent national authorities to the data and their subsequent use for the purposes of prevention, detection or criminal prosecutions concerning offences that, in view of the extent and seriousness of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, may be considered to be sufficiently serious to justify such an interference. On the contrary, Directive 2006/24 simply refers, in Article 1(1), in a general manner to serious crime, as defined by each Member State in its national law.

61 Furthermore, Directive 2006/24 does not contain substantive and procedural conditions relating to the access of the competent national authorities to the data and to their subsequent use. Article 4 of the directive, which governs the access of those authorities to the data retained, does not expressly provide that that access and the subsequent use of the data in question must be strictly restricted to the purpose of preventing and detecting precisely defined serious offences or of conducting criminal prosecutions relating thereto; it merely provides that each Member State is to define the procedures to be followed and the conditions to be fulfilled in order to gain access to the retained data in accordance with necessity and proportionality requirements.

62 In particular, Directive 2006/24 does not lay down any objective criterion by which the number of persons authorised to access and subsequently use the data retained is limited to what is strictly necessary in the light of the objective pursued. Above all, the access by the competent national authorities to the data retained is not made dependent on a prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued and which intervenes following a reasoned request of those authorities submitted within the framework of procedures of prevention, detection or criminal prosecutions. Nor does it lay down a specific obligation on Member States designed to establish such limits.

(…)

65 It follows from the above that Directive 2006/24 does not lay down clear and precise rules governing the extent of the interference with the

fundamental rights enshrined in Articles 7 and 8 of the Charter. It must therefore be held that Directive 2006/24 entails a wide-ranging and particularly serious interference with those fundamental rights in the legal order of the EU, without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary."

1.7. On 17 November 2014 the Cabinet has responded in writing to the invalidation of the Data Retention Directive. In that letter the Cabinet mentioned that the Wbt should be amended in light of the Court judgment. Among other things, that letter states:

"The government is so intending to amend the national legislation in matters of the retention obligation of telecommunication data, so that:

- *the demand by the public prosecutor for the provision of telecommunication data may only be given after a previous authorization by an examining judge. This means that the regulation of article 126n/u of the Code of Criminal Procedure Code of Criminal Procedure will be amended;*
- *The access to the data for the purpose of investigation and prosecution of serious crimes will be differentiated based upon the seriousness of the crime. This means that the regulation of article 126n/u of the Code of Criminal Procedure Code of Criminal Procedure will be amended;*
- *It will be investigated whether the telecommunication data, that are retained for the purpose of investigation and prosecution of serious crimes, could be encrypted so that they are shielded from inspection by unauthorized persons. This may lead to an amendment of the Decision security of telecommunication data;*
- *The providers will be required to retain the data on the territory of the European Union. This means that the regulations of articles 13.2a and 13.5 of the Telecommunnication Act will be amended;*
- *AT* Radiocommunications Agency, addition by provisional judge) (*sic*) *will be given access, as the supervisory authority, into the telecommunications data that are retained or given by the providers, in with an eye towards a better supervision on the processing of the data that are to be retained or destroyed. This means that article 18.7, second paragraph, of the Telecommunication Act will be amended;*

These amendments will be part of an proposed amendment of the Telecommunication Act and the Code of Criminal Procedure Code of Criminal Procedure, that will be given in consultation soon."

2 The Dispute

2.1. Privacy First cs claim, after changing the demand, concisely:
Primarily:
I. the Wbt, at any rate article 13.2a and/or article 13.2 and/or article 13.4 of the Telecommunication Act be rendered inoperative, or at any rate sentence the State to do that;

II. Prohibit the State from requesting data as alluded to in article 13.2a Telecommuncation Act from providers of public telecommunication networks or public telecommunication services, insofar as these matters are in violation of the principles formulated by the judgment of the Court of 8 April 2014;
Subsidiary:
Prohibit the State to enforce the Wbt or parts thereof and request data as alluded to in article 13.2a Telecommunication Act from the providers of public telecommunication networks or public telecommunication services, insofar as this is in violation of the articles 7, 8 and 11 of the Charter, 8 and 10 of the European Convention on Protection of Human Rights and Fundamental Freedoms (ECHR), 10 of the Constitution, 15 of the e-privacy Directive and/or 6, paragraph 1 and 2 of the Treaty on European Union;
More subsidiary:
Prohibit the State to enforce and force providers of public telecommunication networks and public telecommunication services to save and request the data as meant in article 13.2a Telecommuncation Act, so long as the Wbt is not amended as proposed by the government in its letter of 17 November 2014 or the Wbt is repealed by law.

2.2. To that end Privacy First cs argue the following. The Wbt is unquestionably in violation of the European rules and cannot endure. The Wbt implements the Data Retention Directive almost verbatim. The Court has invalided the Data Retention Directive on 8 April 2014 with retroactive effect. The Wbt violates articles 7 and 8 of the Charter in a similar fashion as the Data Retention Directive did.

The Data Retention Directive left some leeway to retain the data of everyone. The Wbt made use of that. The Court condemned the undirected retention of data of all citizens, without differentiation by person, location or data. The retention of all traffic and location data for six to twelve months, irrespective of goal, therefore goes too far. There has to be a limited or targeted selection of those data. There is none in the Wbt. Moreover the Court feels strongly about the fact that there is no prior judicial supervision. Under the Wbt it is still possible for criminal investigators and public prosecutors to get access to the data, without a judicial check beforehand. The Court has furthermore expressed objections against the retention periods, as prescribed in the Data Retention Directive, as there is no differentiation made depending on the use thereof, which purpose they serve or the persons involved and the lack of objective criteria mentioned to limit the retention periods to those strictly necessary. The Court also determined that there are insufficient guarantees that the data are protected against abuse.

The Wbt is furthermore in violation of article 8 ECHR. The *storage* of traffic and location data and the *access* of the national authorities to those data are both independent violations of the right to protection of privacy. The storage is also a violation in the event only a limited part of the stored data is actually used. The retention of large amounts of data about innocent people that the Wbt covers, is a serious violation of article 8 ECHR. From this data it is possible that very precise conclusions may be drawn concerning the private life of the people of whom the data is retained, as the Court also notes. The Wbt provides insufficient safeguards against abuse and arbitrariness and it is insufficiently clear and precise under which circumstances and conditions the authorities may use these measures. For example, the Wbt does not govern that every individual request for access to the data is subject to the supervision of the authorities. What's

more the Wbt is not 'necessary in a democratic society'. The serious breach of privacy is not proportional to achieve its objective, namely to detect serious crime.

The Wbt is also in breach of the right to freedom of expression (article 10 ECHR and article 11 of the Charter). The fact that data of journalists can be requested, leads to the risk that the journalists will avoid certain topics or that sources will no longer dare to contact journalists. Also clients will feel less free to consult their lawyers. There is thus a danger of a "chilling effect". The government forces providers of telecommunication services to violate the fundamental rights of their clients *en masse*. In addition, their freedom of contract and their freedom of establishment is affected.

In the letter of 17 November 2014 the Minister of Security and Justice indeed proposed an Act of amendment, but until that Act will enter into force the Wbt will be enforced as is. It is widely believed that the Wbt with its current content can no longer be enforced. The Department of Advice of the Council of State has made this crystal-clear. This is furthermore supported by the Dutch Data Protection Authority (DPA) and authoritative scholars.

In addition to that the Wbt is hardly effective and largely outdated by continuous technological developments. The necessity and effectiveness of the Wbt after five years of data retention have not been shown. Many other Member States in Europe have abolished their laws based on the Data Retention Directive already or have set aside the obligation to retain the data.

2.3. The State has pleaded a reasoned defense, which will be discussed, insofar as necessary, in the following.

3 The assessment of the dispute

3.1. It is presupposed that the claim is directed at the State as legislator and extends to make inapplicable a part of an Act of Parliament. The civil judge in a provisional proceeding can only make an Act of Parliament or parts thereof inapplicable in the event that and to the extent that this Act is *unmistakenly nonbinding* because it is contrary to a provision that binds anyone stemming from a treaty and/or a decision of an international organization. This criteria flows from article 94 of the Constitution and established jurisprudence (according to Dutch Supreme Court 1 July 1983, NJ 1984, 360) and requires great restraint, even more so as in a preliminary proceeding like this one only a preliminary judgment can be given. This required restraint is based on the division of powers in the Constitution to different organs of state – the separation of powers. Acts of Parliament are determined by the legislator. It is pre-eminently the task of the legislator to take into account and weigh the different interests that are discussed in this case, and in doing so the legislator is awarded a great deal of discretion. There is therefore no place for an independent "full" review by the civil court.

3.2. The state has argued that the criminal court has already explicitly dealt with the legitimacy of the Wbt (Appelate Court Amsterdam 9 May 2014, ECLI: NL:GHAMS:2014:1835 and Appelate Court Amsterdam 27 May 2014, ECLI:NL:GHAMS:2014:2028), so that hardly may be concluded that there is an unmistaken nonbindingness of the Wbt. That argument fails. The Criminal Court

has assessed whether there was a technicality default based on article 359 paragraph 1 Code of Criminal Procedure Code of Criminal Procedure has occurred and whether the interests of the defendants by application of the (revised) Telecommication Act have been breached. The civil court assessment on whether the Wbt is in violation with a provision that binds anyone stemming from a treaty or a decision by an international organization has not taken place in the referred to judgments.

3.3. Privacy First cs have invoked the consideration of the Court in its judgment of 8 April 2014 in which it to substantiate their claims, the judgment in which the Data Retention Directive was invalidated. It is not disputed, however, that the invalidation of the Data Retention Directive by the Court not necessarily implies that the Wbt is also invalid. Due to the invalidation of the Data Retention Directive the Wbt became autonomous legislation that should be assessed on its own merits, in which the considerations by the Court should be involved. It is further noted that the proposed amendments of the Wbt as described in the letter of 17 November 2014 do not play a role in the assessment, as only the current state of legislation should be assessed.

3.4. Article 51 of the Charter determines that the Charter applies where the Member States are implementing Union law. From the case law of the Court it follows that the term 'implementing Union law' within the meaning of that provision must be understood that is the Member States acting within the scope of Union law (among others: Court of Justice EU 30 April 2014, C-390/12, Pfleger). Since the Wbt is an implementation of the so-called e-privacy Directive (Directive 2002/58/EC) and brings with it a restriction of the free movement of services, this Act falls under the scope of the Charter. It should therefore be assessed whether the Wbt – as is claimed by Privacy First cs – is an impermissible violation of articles 7 and 8 of the Charter. The State has not disputed that the Wbt has almost the exact content of the Data Retention Directive, but has – in the judgment of the provisional court rightly so – taken the view that the entire body of relevant national legislation should be included in the assessment of the question whether the Wbt is in accordance with the articles 7 and 8 of the Charter. The objections against the Data Retention Directive as voiced by the Court in its 8th of April 2014 ruling, include after all among other concerns the absence of certain safeguards for the security of and access to the stored data. Those objections could also be overcome by applicable provisions in other national legislation.

3.5. Articles 7 and 8 of the Charter formulate the right to respect for private and family life, home and communications and the right to protection of personal data. Privacy First cs have argued that the mere fact that the Wbt prescribes that telecommunication data of persons are stored already constitutes an impermissible breach of articles 7 and 8 of the Charter. It is firmly established that, as the Court also considers under points 32 through 27 of the judgment, the (in this case by the Wbt) obligation to store data about the communications of persons for a certain period of time is an interference of articles 7 and 8 of the Charter. That is in line with the case law of the European Court of Human Rights, to which Privacy First cs refer. In this case law it is for instance considered that in terms of article 8 ECHR "*The mere storing of data relating to the private life of an individual amounts to an interference within the meaning of article 8 (...). The subsequent use of the stored information has no bearing on that finding.*" (ECtHR 4 December 2008, S. and Marper, applnos 30562/04 and 30566/04). Privacy First cs. therefore are correct in stating that the *use* of the data is an independent, far-

reaching interference is with the aforementioned rights. Insofar as Privacy First cs however argue that interference on its own is unacceptable, that argument is not followed. It should be assessed whether there interference is justified and proportional.

3.6. In that context the parties are disputing the necessity and effectiveness of the retention obligation that is prescribed by the Wbt. With respect to that it is postulated that this dispute is pre-eminently within the discretion of the legislator, who should weigh all of the interests against one another, so that the provisional court only marginally assess this point. The Court has held that the suppression of serious crime is of paramount importance to ensure public safety, that its effectiveness may substantially depend on the use of modern investigation techniques (consideration 51) and that the data that should be retained provides for extra possibilities to clear up serious crime cases (consideration 49). In addition the State in these proceedings has adequately established that the detection of certain types of crimes rely almost exclusively on the use of historical telecommunication data, based on the fact that more and more crime is committed on or using the internet. The State has argued, without being challenged, that some of its extensive criminal cases could not have been resolved without the use of data retention. The starting point is therefore that the data retention obligation is necessary and effective.

3.7. The dispute of parties is further focused on the question of the Dutch legislation has taken adequate steps to counter the objections that have led the Court to decide to invalidate the Data Retention Directive. Similar to the Data Retention Directive the Wbt applies to all people who make use of electronic communication services without any limitation, and thus applies to people for whom there is no indication that their behavior is connected to serious crime. There is also no connection required between the data that have to be retained and a treat to public safety (considerations 79-59 of the judgment). Other than Privacy First cs argue, it cannot be deduced form the judgment of the Court that such a wide retention obligation is in any event disproportional to its purpose. After all, the Court then assesses the question whether the Data Retention Directive provides for enough safeguards to access the retained data. In that assessment the Court, "having regard to al the foregoing considerations" (consideration 69), concludes that the legislator has overstepped the boundaries set by the principle of proportionality. From that it follows that the enumerated objections considered in conjunction with one another have led to that judgment.

3.8. The foregoing is without prejudice to the assessment that has to be made whether the interference with articles 7 and 8 of the Charter is sufficiently precise framed by the provisions that safeguard that they truly are limited to the absolute necessary. In that respect it is noted that a limitation of the data that have to be stored to those data of suspected citizens is not conceivable in light of the purpose of the Wbt, the effective tracing of serious crime. Indeed, in case of a *first offender* it is not possible to make a distinction in advance between suspect and non-suspect citizens. The necessity to provide for safeguards and guarantees regarding access to those data is however all the greater as we are dealing with a very extensive interference, so high standards should be set.

3.9. The State has correctly argued that providers of telecommunication services in the Netherlands, based on the Decision security data telecommunications, have to offer a high level of protection and security and that the

Radiocommunications Agency and the Data Protection Authority have to supervise this. To that extent the objections voiced against the Data Retention Directive by the Court in consideration 67 have been rebutted. However, from consideration 69 it should be derived that a provision that the concerned data should be retained on the territory of the Union is an essential component for the protection of the people in the processing of personal data, since only with such a provision it is fully ensured that an independent authority on the basis of EU law can supervise the requirements concerning protection and security solutions. Such a provision is missing in the Wbt. The State has also acknowledged that in practice (certain small) providers retain their user data outside of EU territory.

3.10. Moreover – according to the Court in consideration 60 of the judgment – the legislation should include objective criteria that limit the access of the authorized national authorities to the data and the later use of these data with the purpose of preventing, investigating and criminally prosecuting interferences that are deemed sufficiently serious, so as to justify the interference with the fundamental rights as recognized by articles 7 and 8 of the Charter. The provisional court is of the opinion that this not the case in the Wbt. The Wbt provides for a clear delineation because consultation of the data is limited to the investigation and prosecution of criminal offences for which remand is permitted or for terrorism, but this category also includes criminal offences that not sufficiently serious to justify the interference. The provisions of the Data Retention Directive were a response to the terror attacks in London and Madrid in 2004 and 2005. The material purpose/scope of the Data Retention Directive, as thusly that of the resulting Wbt, consisted of a guarantee that certain data be available for the purpose of combatting *serious* crime. Offenses for which remand is allowed, include offences which carry a penalty of at least four years. The State has argued that they do not lightly request the data and that in instances such as a bike theft (also an offence for which remand is permitted) no data will be requested. Fact is however, that the possibility to do just that exists and that there are no safeguards in place that limit the actual access to the data which is strictly necessary for the combatting of (only) serious crime.

3.11. The foregoing is all the more important considering that the Wbt and related regulations do not require a prior authorization by a judicial authority or independent administrative body in order to access of the retained data. Different from that which is argued by the State, the office of public prosecution cannot be considered an independent administrative body. That the Court has considered this as a compelling objection can be derived from the words “above all” in consideration 62 of the judgment.

3.12. All this leads to the conclusion that the Wbt in its current form is a violation of the rights protected by articles 7 and 8 of the Charter which is not limited to the absolute necessary and thus needs to be qualified as an unacceptable. In light of this the Wbt is unmistakably nonbinding. The provisional court is aware that making the Wbt inoperable may have profound implications for the detection and prosecution of offences. That however does not justify the continuation of the aforementioned violation. That the consequences of such inoperability may be irreversible also does not stand in the way of providing the requested interim provision. The primary claim by Privacy First cs, as formulated under I, is thus awarded. Hence, Privacy First cs have no interest in awarding that which was

claimed under II. This is so because making the Wbt inoperable leads to the legal basis for the request of the referred data is lapsed.

3.13. The State, as the unsuccessful party, be ordered to pay the costs of these proceedings, as well as (partially conditional) subsequent costs.

4 The ruling

The court in summary proceedings:
- Renders the Act retention telecommunication data inoperable;
- Orders the State to pay the costs of proceedings incurred by the claimant (…)
- Declares this judgment thus far provisionally enforceable
- Dismisses all other applications

This judgment was rendered by mr. G.P. van Ham, pronounced in public on 11 March 2015