DATA PROTECTION, PRIVACY AND EUROPEAN REGULATION IN THE DIGITAL AGE

EDITED BY
TOBIAS BRÄUTIGAM AND
SAMULI MIETTINEN

FORUM IURIS

Helsingin yliopiston oikeustieteellisen tiedekunnan julkaisut

© Bräutigam, Tobias ja Miettinen, Samuli (toim.): Data Protection, Privacy and European Regulation in the Digital Age

ISBN 978-951-51-2530-9 (painettu)
ISBN 978-951-51-2531-6 (pdf)
ISSN 1456-842X (painettu)
ISSN 2342-8996 (verkkojulkaisu)

Unigrafia
Helsinki 2016

Fundamental rights compliance and the politics of interpretation:

Explaining Member State and court reactions to Digital Rights Ireland

Niklas Vainio*

INTRODUCTION

The EU introduced the Data Retention Directive ("the Directive")[1] after the terrorist attacks in Madrid and London in 2004. The purpose of the Directive was to obligate telecommunication service providers to retain specified phone and internet-related metadata in order to ensure that the data were available for the purpose of the investigation, detection and prosecution of serious crime (art. 1(1) of the Directive).

The Directive was heavily criticised for its strong interference with fundamental rights, particularly the right to privacy and the right to protection of personal data.[2] It required Member States to oblige telecommunications companies to store all traffic data about all phone calls, internet access and e-mail communications that took place in their network. The data was to be retained for a period of 6–24 months, depending on the national implementation of the Directive.[3] Access to the data was not regulated in the Directive, as it is outside the jurisdiction of the EU. The European Data Protection Supervisor,[4] the Article 29 Working Party[5] and various digital rights organisations expressed strong concerns about the necessity and proportionality of the proposal.

The constitutionality of the data retention regime was challenged in several Member State courts, with each challenge leading to an annulment of the domestic retention law.[6] An EU-level judgment was finally given in April 2014 when the Court of Justice of the European Union ("the CJEU") gave its ruling in the joined cases of *Digital Rights Ireland* and *Seitlinger*.[7] The judgment declared the Directive invalid on the grounds that it violated the rights to privacy and data protection and exceeded the limits of what

* LL.M., M.Sc., University of Turku. E-mail: niklas.vainio@utu.fi.

was acceptable in the view of the principle of proportionality. Although counted as a victory by privacy advocates, the ruling has not led to the uniform consequences which one might expect. Several court decisions were given after the ruling, again striking down the national data retention laws, yet governments in other Member States have taken a completely different direction, either by keeping their data retention laws unchanged, or even by expanding them.

In this chapter, compliance of the Member States with the judgment is studied. The purpose of directives and the interpretations given by the CJEU is to harmonise the law in the Union. This begs the question: Why do the readings of the Directive and judgment lead to such different outcomes? Also, as long as the status of data retention remains unclear—with some Member States still retaining data—does the Charter of Fundamental Rights effectively protect the rights to privacy and data protection?[8]

THE CJEU'S JUDGMENT IN *DIGITAL RIGHTS IRELAND*

The Directive required the retention of data detailing the time of telephone or e-mail communications, their participants and possibly a location of a mobile phone at the time (this type of information is referred to as "meta-data"). Retention of the content of the communications was not allowed.[9] Although the metadata relating to a single call alone does not amount to any major interference with the privacy rights, when collected into a database of billions of calls, different privacy issues arise. The CJEU noted, at paras. 26–27, that such a database makes it possible to create profiles of citizens and draw conclusions concerning their private lives like habits, permanent or temporary places of residence, regular movements, activities, social relationships and social environments. For this reason, the court concluded in paras. 35–36, that the retention of data constitutes an interference with the Charter of Fundamental Rights, art. 7 (right to privacy) and art. 8 (data protection).

The obligation to retain communications metadata was broad: it applied to all means of electronic communication and all users, thus entailing "an interference with the fundamental rights of practically the entire European population" (para. 56) without "any differentiation, limitation or exception" (para. 57). Data retention is a "particularly serious" interference with the right to privacy and data protection (para. 37). The knowledge of retention and use of the data without the users having been informed is "likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance" (para. 37). Because

the interference is particularly serious, the review of the discretion accorded to the EU legislature must be strict (para. 48).

The court found problems with the proportionality of the Directive. The following shortcomings are mentioned in the judgment:[10]

(1) The scope of retention had been wide and indiscriminate, covering the whole population (para. 56);
(2) Any evidence of a person's link to serious crime had not been required (para. 58);
(3) Any relationship between the data and a threat to public security had not been required (para. 59);
(4) Retention had not been restricted to a particular time period, geographical area, and/or to suspects of serious crimes or persons whose data would contribute to the prevention, detection or prosecution of serious offences (para. 59);
(5) The Directive had not in any way accounted for conditions when particularly high requirements for privacy were in place, for example when a medical doctor or an attorney communicates with a client (para. 58);
(6) The Directive had not established any connection between the retention time and the usefulness of the data for the stated purposes (paras. 63–64);
(7) The Directive had not provided any rules for access and use, nor had it provided substantive and procedural conditions for access (paras. 60–61);
(8) The number of persons authorised to access and use the data had not been limited to that which was strictly necessary (para. 62);
(9) Neither an independent nor a court review had been required to access the data (para. 62);
(10) The Directive had not required the data to be retained within the EU, which would have ensured the control of compliance with the rules relating to protection and security by an independent data protection authority, as required by art. 8(3) of the Charter (para. 68);
(11) There had not been any requirement which had specified that the persons who were the target of data retention be notified (para. 37);
(12) The Directive had not specified measures that ensured effective security and protection against the risk of abuse and unlawful access and use of the data (para. 66); and
(13) The Directive had not ensured irreversible destruction of the data at the end of the retention period (para. 67).

The judgment did not specify if this was a list of changes that would make data retention proportional or just an observation of the problems in the Directive. Further, the judgment did not specify whether precautionary blanket retention is even legally permissible under the Charter (which is, essentially, the question asked by the Swedish Administrative Court of Appeal in its referral to the CJEU—see below).

The conclusion of the court was that the wide-ranging interference of the Directive was not properly limited to what was strictly necessary (para. 65) and therefore the Directive failed the requirements of art. 52(1) of the Charter and must be declared invalid.

REACTIONS TO THE JUDGMENT

At first glance, the court's response to the referral resolved questions regarding the fundamental rights status of data retention. Many expected that the court's ruling would lead to a repeal of data retention laws around Europe. However, because of the unresolved issues—most importantly the question of whether general blanket retention might ever be lawful—this did not happen. As seen above, the judgment did not rule retention illegal as such, but instead gave a long list of problems in the Directive which, depending on the reading, is either a list of reasons for annulment or a list of requirements to be satisfied to make data retention proportionate.

The status of data retention legislation in the Member States is the following (as of May 2016):[11]

Old law in force	Cyprus, Czech Republic, Denmark, France, Croatia, Hungary, Portugal, Sweden
Invalidated by a national court	Austria, Belgium*, Bulgaria*, Germany*, Slovenia, Netherlands*, Poland, Romania, Slovakia * new legislation on data retention adopted after the invalidation or in process of adoption
No formal invalidation, but new or amended data retention legislation	Estonia, Spain, Finland, Ireland, Lithuania, Luxembourg, Latvia, Malta, Poland, the U.K.

Three kinds of legislative and judicial reactions to the judgment can be distinguished:

(1) court actions based on a strict reading that lead to invalidation of the domestic laws;

(2) governmental and legislature actions and non-actions based on a permissive reading of the judgment that maintain the data retention obligations or expand them; and
(3) actions where the concerns of the court were addressed while still maintaining some form of generalised, blanket retention obligations in place.

Member State's constitutional courts seem to follow the stricter reading of the judgment. All of them are, more or less, in line with the CJEU's reasoning. These judgments and their national particularities are described below. After that, governmental reactions in selected Member States are grouped and studied according to what seem to be the major influencing factors in the way that they interpret the *Digital Rights Ireland* judgment.[12]

INVALIDATION BY COURTS

In many Member States, the question of the legality of blanket retention was taken to the constitutional court. Each court operates within the framework of its national constitution and anchors its assessments accordingly, some emphasising the European Convention on Human Rights and Fundamental Freedoms ("the ECHR"), some the national constitution. All, however, follow the general reasoning of the CJEU.

AUSTRIA

The Austrian Constitutional Court reacted two months after having received the answers to its referral.[13] According to the court, Austrian data retention laws are contrary to the right to data protection and the right to privacy as protected in the national constitution and the ECHR. Thus, the national law was ruled invalid, effective immediately. The court described data retention as a "massive interference" with the right to privacy. The challenged provisions of the domestic law did not meet the requirements of proportionality because the definition of the retention obligation was too vague and the provisions regarding access to data and its deletion did not meet the constitutional requirements.

SLOVAKIA

The Constitutional Court of Slovakia gave its judgment on the domestic data retention laws in April 2015.[14] The primary norm of reference for

the court was the national constitution, but, as described by Husovee, the court relied on the case law of the CJEU to "determine the content of the national constitutional provisions."[15] The court found that retention and subsequent access violated the national constitutional provisions on privacy (Constitution of the Slovak Republic, arts. 16(1) and 19(2)), protection of personal data (art. 19(3)) and secrecy of correspondence (art. 22) and the ECHR, art. 8.

The court's proportionality analysis seemed to follow that of the CJEU's—it mentioned, for example, the "serious interference with the right to informational self-determination" and the "great and unpredictable number of people" in its scope.[16] Also mentioned is the blanket nature of retention and the fact that retention is not limited based on time, geography or group.[17] The court also found access provisions problematic because the rules on access were of insufficient quality and allowed overuse of the retained data in cases of less serious crime. The court mentioned some changes that would constitute a "somewhat more proportionate interference" but left it open as to whether those would save the legislation or whether, even if the changes were introduced, the indiscriminate nature of the retention would violate the constitution.[18] Interestingly, the court also emphasised the positive obligation of the State to create favourable conditions for citizens to enjoy their privacy.[19] As was requested by the court, the government has proposed a law that defines, in detail, the conditions under which data can be retained, stored or requested by State bodies. Use of the data is limited to the most serious crimes, such as terrorism.[20]

SLOVENIA

The Constitutional Court of the Republic of Slovenia issued its judgment in July 2014[21] in which it annulled the data retention provisions of the national law and ordered immediate deletion by the teleoperators of the retained data. The court held the retention as disproportionate for four reasons:

(1) blanket retention of data constituted a breach of the rights of a large proportion of population without legal justification;
(2) it made anonymous communication impossible, which the court had held particularly problematic in certain situations (*e.g.* calling for help in instances of mental distress);
(3) arguments for selective retention periods (8 months for internet-related and 14 months for telephony-related data) were not provided or elaborated on in the legislative materials; and
(4) the use of retained data was not limited to serious crime.[22]

ROMANIA

The Romanian Constitutional Court struck down the national data retention statute in 2009, finding that mass retention of data violated the principle of proportionality and "emptied" the right to privacy, making the right only theoretical and illusory.[23] A new law was adopted in 2012, apparently in fear of sanctions from the European Commission for the failure to implement the Directive. The new law was similar to the old one and was accepted, despite receiving heavy NGO criticism and being in conflict with the Constitutional Court's decision.[24] Two months after *Digital Rights Ireland*, on 8 July 2014, the Constitutional Court again ruled against data retention on similar grounds to those in the 2009 judgment, while also criticising the lack of adequate judicial approval and disproportionate access rules.[25]

BULGARIA

In 2008, the Bulgarian Supreme Administrative Court gave a judgment repealing the national data retention law. In 2010, a new law requiring data retention for a period of one year was adopted to implement the Directive.[26] In its judgment of 12 March 2015, the Constitutional Court ruled that the provisions in the domestic law which required retention were unconstitutional. The court stated that the legislature had exceeded its jurisdiction because the constitution only allowed for a limitation of the confidentiality of correspondence in the case of serious crime. The court found that the access was given to too wide a group of authorities and that they were given the power to order an extension to the retention period without any judicial review. Access required a court warrant, but the constitutional court found that the level of specificity required from the applications was insufficient.[27]

In its proportionality assessment, the Bulgarian Constitutional Court stated, echoing the German Federal Constitutional Court, that blanket retention as such is not prohibited, but because data retained for 12 months could be used to create profiles of citizens and their lives, it was beyond what was necessary to achieve the aims of the legislation.[28]

Soon after the judgment, the parliament passed a number of amendments to the law attempting to resolve the problems found by the court. The new law allows for the use of the data in cases of serious crime only, which conforms to the e-Privacy Directive,[29] art. 15. The authorities which have access are specified in the law, although the list remains long, and access requires a court warrant. However, the requirements regarding

necessity of access are still inadequate. The law reduced the retention period to six months (with a possibility of extension by three months).[30]

NETHERLANDS

In November 2014, the Dutch government announced that it would continue to retain telecommunications data but would make some changes to the law in response to the *Digital Rights Ireland* judgment. The government argued that although the Directive was ruled invalid, the judgment did not imply that national legislation implementing the Directive was invalid and that the Dutch law "already contains safeguards that exceed those of the data retention directive."[31] As proof of necessity of the retention regime, the government cited examples of two robbery cases, a rape case and a child abuse case where data retention played a role or could have helped in solving the case. The government did its best to argue that although CJEU stressed the need for link to serious crime in *Digital Ireland* (para. 58), access to communications data is important in the investigation and prosecution of crimes and it is not possible to differentiate between suspected and unsuspected citizens beforehand. According to the government, the CJEU judgment was made "taking all considerations into account", which would mean that although data retention is a very serious interference with the right to privacy, the seriousness of that interference can be mitigated "by appropriate guarantees and safeguards". To provide such guarantees, the government proposed to amend the existing law to—

(1) require court approval for access to the data,
(2) access to the data will be differentiated based on the seriousness of the crime,
(3) require encryption of the data to enhance its security,
(4) require retention of the data within EU, and
(5) have the Telecom Agency oversee the processing and erasure of the data by the providers (with the side effect that the Agency has access to the data).[32]

A case against the State was initiated in the District Court of The Hague by a group of civil society organisations and internet companies. The plaintiffs requested that the court forbid the State from enforcing the data retention rules or gaining access to the retained data, arguing that data retention and access violate both the Charter of Fundamental Rights (as described by the CJEU) and the ECHR, art. 8. In its judgment of 11 March 2015, the court assessed the national law against the Charter using the CJEU judgment as a template. The court emphasised the CJEU's finding that data retention legislation should include objective criteria which limits access to the data

and its use to the prevention of, investigation of and criminal prosecution of offences that are deemed sufficiently serious. The Dutch law allowed access and use for minor criminal offences such as a bicycle theft. The court was not satisfied with the State's statement that the data was not requested in minor cases such as these. Regardless of the assurances by the State, the possibility of access to the data existed in the law. There were insufficient safeguards in place to limit actual access to the data only to that which was strictly necessary for the combatting of serious crime. Furthermore, the court noted that the law did not require prior authorisation by a judicial authority or an independent administrative body in order to gain access to the retained data. The court did not accept the claim of the State that the office of public prosecutor could be considered an independent administrative body. For these reasons, the court found the national law in violation of the rights protected by the Charter, arts. 7 and 8 and declared the law invalid.[33]

Several operators have stopped retaining data after the judgment.[34] The Dutch government has chosen not to appeal the judgment and plans to re-introduce a data retention law. The current draft of the law is essentially similar to the one struck down by the court.

BELGIUM

The Belgian data retention law was struck down by the Constitutional Court of Belgium on 11 June 2015. The judgment followed the argumentation of the CJEU in *Digital Rights Ireland* closely. It even explicitly states that, for the same reasons as those that led to the CJEU to declare the Directive invalid, the Belgium legislature had exceeded the limits imposed by the principle of proportionality with regard to the Charter, arts. 7, 8 and 52(1).[35] As additional arguments, the court referenced the principles of equality and non-discrimination, echoing the CJEU's criticism in para. 58 of *Digital Rights Ireland* (requirement of a link to crime). This would seem to advocate a targeted retention approach.[36]

The government of Belgium is keen to have data retention back on the EU agenda and is planning a new law, possibly in co-operation with the Dutch and Luxembourgian governments.[37]

THE UNITED KINGDOM'S EXPANSIONIST STRATEGY

In the U.K., the government of the day was quick to react to the judgment. The response represents a totally opposite reading of the judgment compared to that of the constitutional courts.

Warning of "grave" consequences for security and crime prevention if the government did not act, the cabinet proposed an "emergency" law, the Data Retention and Investigatory Powers Act ("DRIPA") using a highly unusual fast-track procedure. According to the then-Prime Minister David Cameron, such an exceptional measure was necessary to protect existing interception capabilities in the fear that telecommunication service providers will stop retention and delete the data.[38] The Bill was adopted a mere three days later.[39]

The new law was basically an attempt to maintain data retention, just under a different name. The system enacted by the new law is similar to the one that was implemented under the Directive, except that it does not use the same language as in the Directive. Under DRIPA, data retention is based on retention notices. The Secretary of State may give a public telecommunications provider a notice to retain relevant communications data if the Secretary of State considers that the requirement is necessary and proportionate for one or more of the purposes defined in the Regulation of Investigatory Powers Act 2000. Section 1(5) specifies a maximum retention period of 12 months, but the law does not lay down other binding limitations regarding the scope of retention.

According to critics, DRIPA actually went further than merely maintaining the data retention regime[40] and fails to meet the requirements of the CJEU judgment. The civil rights organisation Liberty used strong language in its critique of the bill—according to Liberty, the bill "doesn't even pretend to comply with the CJEU judgment."[41] Instead, it sought to re-enact a mandatory communications data retention regime for the entire population for up to 12 months, without even limiting collection to cases involving the prevention or detection of serious crime. The Act allows access to the data for a broad group of public authorities and many can do so without the need to obtain prior judicial authorisation.

As DRIPA is practically the Directive re-implemented, but with the reference to the annulled Directive dropped, can such legislation be in compliance with the Charter of Fundamental Rights? The government argues that all the problems raised by the CJEU in *Digital Rights Ireland* are addressed by the "robust safeguards" in the national regime.[42] Yet, some of the gravest problems seem not to have been addressed at all. For example, the law does not restrict retention to cases with a link to serious criminal

activity or terrorism as the CJEU required in para. 58 of its judgment. Independent supervision of access to the data has not been mandated (per para. 68) and there are no hard limits on the length of retention period (per paras. 63–64).[43] The differences between the original law and the renewed data retention law are so minimal that it is difficult to argue that DRIPA would meet the requirements set out in the ruling. In this light, it is easy to see some justification in Liberty's accusation that the bill "shows utter contempt" for the principle of Rule of Law by "attempting to overrule rather than comply with a Court judgment".[44]

THE CRITICAL HIGH COURT

DRIPA was challenged in the High Court of England and Wales.[45] Claimants, two of whom were MPs, argued that DRIPA, s.1 and the related Regulations were invalid because they violated the Charter, arts. 7–8, as expounded in *Digital Rights Ireland,* and the ECHR, art. 8.

Citing the Charter, art. 51, the court held that since the EU had legislated extensively in the area of data protection, the U.K. is "implementing EU law" with DRIPA and therefore it has to respect the Charter rights.[46] While the court agreed with the government that the CJEU in *Digital Rights Ireland* only ruled on the validity of the Directive, not on any domestic regime, similar principles applied when assessing DRIPA. The Directive exceeded the limits of proportionality and lacked sufficient safeguards against risk of abuse and unlawful access. According to the High Court, "it must follow that in the view of the CJEU a domestic statute in identical terms would have had the same failings."[47]

While the rules regarding access to retained data fall outside the competence of EU, the court argued that rules on access nevertheless influence the legality of a retention regime, stating that "legislation establishing a general retention regime for communications data infringes rights under Articles 7 and 8 of the EU Charter *unless* it is accompanied by an access regime (laid down at national level) which provides adequate safeguards for those rights."[48] [Emphasis in original.]

The government argued that the ECtHR had approved the U.K.'s access regime under RIPA in *Kennedy v U.K.*[49] so the lack of access safeguards in DRIPA could not be considered a problem.[50] The court dismissed the argument that *Kennedy* requires the "reading down" of the protection in the Charter so as to match ECtHR case law for two reasons. First, the ECHR, art. 8 and the Charter, arts. 7 and 8 do not match because the Charter, art. 8 introduces a separate data protection right. Secondly, ECtHR rulings form a floor, not a ceiling, for rights protection.[51]

According to the court, the *Digital Rights Ireland* judgment lays down three clear requirements:

(1) only strictly necessary limitations can be made,
(2) a general retention regime must expressly provide that the access to and use of the data is "strictly restricted to the purposes of preventing and detecting precisely defined serious offences or of conducting criminal prosecutions relating to such offences", and
(3) access must be made "dependent on a prior review by a court or an independent administrative body".[52]

Because DRIPA failed to satisfy these requirements, the court declared that s.1 was inconsistent with the EU law, effective after 31 March 2016.[53]

THE DOUBTFUL COURT OF APPEAL

The government appealed the judgment to the Court of Appeal, which expressed doubts as to whether the CJEU intended to lay down a list of mandatory principles with which the Member States should automatically comply. The court held that the CJEU "was not laying down specific mandatory requirements of EU law but was simply identifying and describing protections that were entirely absent from the harmonised EU regime." [54] According to the Court of Appeal, the absence of safeguards was the reason CJEU found the Directive unlawful and the list of problems included in the judgment was not a list of requirements.[55] Moreover, the Court of Appeal's interpretation of the scope of the Charter was remarkably narrower than the High Court's. According to the Court of Appeal, national laws governing access to retained data by the police and other law enforcement bodies were not "implementing EU law" and therefore fall outside the scope of the Charter.[56] The court was concerned with the fact that the CJEU's requirements for the prior authorisation were stricter than those of the ECtHR.[57]

The court referred the case to CJEU, asking two questions:

"(1) Did the CJEU in *Digital Rights Ireland* intend to lay down mandatory requirements of EU law with which the national legislation of Member States must comply?

(2) Did the CJEU in *Digital Rights Ireland* intend to expand the effect of Articles 7 and/or 8, EU Charter beyond the effect of Article 8 ECHR as established in the jurisprudence of the ECtHR?"[58]

INVESTIGATORY POWERS BILL

While the referral to the CJEU is pending, the U.K. government has proposed an even broader surveillance legislation. The proposed Investigatory Powers Bill makes further changes related to data retention obligations and surveillance powers. The Bill would expand retention obligation to include IP addresses or host names of internet services accessed. This would cover the host name of a web service (such as bbc.co.uk) but not any specific location within that service.[59] Oversight of interception and retention would be strengthened.

NORDIC LEGALISM

Government reactions in the Nordic countries represent an approach that can be called "legalist." Like the U.K. government, Nordic countries justify blanket data retention by reference to the robustness of the legal safeguards in national legislation. Nordic countries have a long tradition of legalism and strong experience of precise law making. The presupposition of these governments seems to be that precise limitations and well-defined safeguards provide enough balance to mass-surveillance to justify blanket retention.

SWEDEN

After the *Digital Rights Ireland* judgment, some Swedish telecommunication service providers announced that they had stopped retention and deleted all retained data.[60] The oversight authority, the Swedish Post and Telecom Authority ("PTS") initially announced that it would not take any action against the providers[61] but, in August 2014, it changed its policy, requiring some providers to resume retention after the government had come to the conclusion that the Swedish law had no difficulty in meeting the requirements of the Union law.[62]

Operator Tele2 refused to follow the new policy. PTS ordered Tele2 to comply,[63] but this order was challenged by the operator. The Administrative Court in Stockholm rejected the complaint, but Tele2 appealed. In April 2015, the Administrative Court of Appeal in Stockholm (*Kammarrätten i Stockholm*) decided to refer the issue of data retention to the CJEU once again. This time, the court is essentially asking if blanket data retention is compatible with the e-Privacy Directive (2002/58), art. 15(1) in the context of Swedish implementation.[64] The court will have to consider the

proportionality of access provisions which, in some cases, allow access with only a suspicion of a crime and without a prior court review.[65]

FINLAND

The Constitutional Law Committee of the parliament reviewed the data retention requirements of the Finnish law as part of larger law reform.[66] Although the Committee found difficulties, especially with the requirements of para. 58 of *Digital Rights Ireland* (link to serious crime), it left the door open for data retention, arguing that there is no obstacle to it, provided the proportionality requirements are met "in other ways"—although it did not specifying what this could mean in practice. The Transport and Communications Committee[67] argued that the *Digital Rights Ireland* judgment does not prevent Finland from having national data retention legislation because the proposed system would be narrower and contain better legal safeguards than the Directive since the scope of obliged providers and the list of data types were narrower. Currently, the Finnish government is preparing surveillance legislation that would allow intelligence authorities search-term based access to internet data. The regime would require a constitutional amendment because the current Finnish Constitution does not permit limitation to the right to privacy on precautionary security grounds.[68]

DENMARK

The government has released a report[69] in which it argues that no major changes need to be made to the data retention legislation. The government notes that, with regard to the link-to-crime requirement, the domestic law is equal to the Directive, but other criticisms do not apply to the Danish implementation. For instance, the Danish law restricts the use of the data to serious crime cases, defined primarily by reference to the prison term of the crime (which has to be six years or more).[70] The government concludes that blanket data retention, as such, is not a violation of the Charter and, as the Danish law has good legal safeguards against the abuse of the data, the domestic law does not violate the Charter.[71] The Danish implementation, however, had expanded data retention beyond the requirements of the Directive to include "session logging", where the internet service providers are required to retain data on the internet connections from a user's computer. The usefulness of session logging has been questioned and the Ministry of Justice decided to repeal the session logging obligation.[72]

CENTRAL AND EASTERN EUROPE: EXTENSIVE SURVEILLANCE

Central and Eastern Europe ("CET") has a history of State surveillance and oppression. Interestingly, some of the most invasive implementations of the Directive still come from that corner of the EU. On the other hand, some constitutional courts of the CET States have been the most fervent defenders of constitutional rights against the supremacy of EU law.[73] For example, the first implementation of the Directive in Bulgaria was invalidated by the Supreme Administrative Court in 2008 because the law allowed authorities direct access to the retention database without a court review.

POLAND

The Polish data retention law of 2009 allows access for a large group of authorities ranging from law-enforcement to intelligence agencies and tax authorities. Retention time is the longest that was allowed by the Directive (two years). The law does not limit use of the data to the investigation of serious crimes and the data can also be used for crime prevention purposes, a purpose that was originally excluded in the Directive (art. 1(1)). Law enforcement and secret services are empowered to access billing and location data without any judicial or other independent control.[74]

The powers are used extensively. According to a European Commission evaluation report on data retention, in 2009, Polish authorities requested access to the data 1m. times, which is approximately half of the combined amount of the 14 Member States that provided numbers.[75] In 2011, this number had already risen to 1.85m.[76] A complaint was submitted in 2011 to the Polish Constitutional Tribunal questioning the powers of law enforcement agencies to access the transmission and location data that are retained under the Polish data retention legislation.[77] The Tribunal gave its ruling after the *Digital Rights Ireland* judgment, ruling that the domestic data retention law must be amended to add more safeguards, such as a closed list of purposes of access, additional protection of data under professional secrecy, and strict rules on deletion of data which are not necessary. Poland has since adopted a new data retention law which, according to critics, lacks an independent control mechanism, still does not limit access to only serious crime and provides for an imprecise and discretionary period of retention.[78]

BULGARIA

After the 2008 judgment of the Supreme Administrative Court, a new law was adopted to restore data retention, which was again annulled in 2015 by the Constitutional Court. The Constitutional Court's decision was not accepted by the majority of the Bulgarian parliament, which made some quick amendments to the law using an "express track" procedure in just under two weeks after the court's decision. Under the amended law, the data retention period is shortened to six months and use of the data is restricted to "national security" and "serious crimes". Court permission is required to access the data and each request is logged in a database. Destruction of the data is overseen by the data protection supervisor.[79] While these amendments probably made the law more proportionate, the fundamental problem of the law—blanket retention—still remains.

GERMANY: ADDRESSING CONCERNS AT HOME AND AT CJEU

The German Federal Constitutional Court annulled the German data retention law in 2010 on the grounds that the law did not meet the requirements of proportionality.[80] The government argued that Germany remained obligated to implement a national data retention law to give effect to the Directive which was still in force. The Federal Ministry of Justice presented, in June 2011, a draft law that would re-implement data retention. The draft proposed a "Quick Freeze Plus" model. In this model, law enforcement authorities could order an operator to retain specific traffic and location data if they had reasonable suspicion that a serious crime had been committed. In addition, data on the use of IP addresses by customers would be retained unconditionally, but only for seven days.[81] The Minister of Justice that proposed the law, Sabine Leutheusser-Schnarrenberger of the liberal party FDP, was actually one of the 35,000 plaintiffs in the constitutional complaint that had just been resolved by the Constitutional Court.[82] The Quick Freeze approach was also the model proposed by civil society organisations and critics of data retention.

The proposed Quick Freeze model was rejected by the Federal Ministry of Interior, which, at the time, was led by a minister from the conservative Christian Social Union ("CSU"). The Ministry of Interior proposed a data retention law in May 2012 with a retention period of six months. This proposal was refused by the Ministry of Justice. There were no further developments during the rest of the legislative period (2009–2013).

After the elections in 2013, a governing coalition of conservatives (the Christian Democratic Union ("CDU") and the CSU) and social democrats ("SPD") was formed. According to the coalition agreement, the government would introduce domestic legislation to re-implement the Directive so as to avoid the non-implementation penalties that it was facing after the constitutional court judgment.[83] Data could be used only in cases of serious crime and if approved by a judge. Storage of the data would also be limited to servers located in Germany. The coalition partners also agreed that they would work at the EU level to shorten the retention time in the Directive to three months.[84] In April 2014, the CJEU struck down the Directive. After this, there was no more pressure from the EU to re-implement data retention. However, the idea was brought back to the table after the Charlie Hebdo attacks in Paris in January 2015. The Federal Ministry of Justice, this time lead by an SPD minister, presented yet another bill[85] to the parliament in June. The bill passed both houses during October and November 2015.[86]

There are major changes in the new law. The retention period has been reduced from six months to between four and ten weeks, depending on the category of the data. The data can be accessed if a warrant is granted by a judge. A warrant can be granted if the suspected crime falls within the catalogue of crimes defined in the law and is considered serious in the particular case, and if access can be considered proportionate in relation to the needs of the criminal investigation. The categories of retained data have been restricted. E-mail data is no longer retained. New measures to ensure data security include logging of access (Telekommunikationsgesetz, §113e); use of encryption (§113d, Abs. 1, Nr. 1); storage of data in separate devices (Nr. 2); disconnecting storage devices from the internet (Nr. 3); and the requirements the data processing facilities may only be accessed by specifically appointed persons (Nr. 4), and that access always requires two specifically appointed persons (Nr. 5). Specific sanctions for non-compliance have been defined. Data of persons under a professional secrecy obligation (lawyers, doctors *etc.*) is still retained, although access to it is limited.[87] These changes probably give the law a better chance of surviving the proportionality assessment that it will soon face, since several complaints against the law have already been filed in the Constitutional Court.[88]

The new law seems, at first glance, to be a serious effort to meet the requirements set by the Karlsruhe and Luxembourg courts. It does not, however, address the major issue raised by the CJEU in paras. 57–59 of *Digital Rights Ireland*: blanket retention of all users of telecommunication without any limitation based on suspicion, geography, time or group.

Another concern related to EU law is that the law requires that all the retained data is stored exclusively in Germany (§.113b, Abs. 1). This is obviously a limitation to the freedom to provide services within the meaning of the Treaty on the Functioning of the European Union ("the TFEU"), art.

56. However, the TFEU permits exceptions to this principle on grounds of public policy, public security or public health in art. 52(1).

The government argues that in this case the restriction is necessary—

> "in order to guarantee the requirements of data protection under Basic Law and data security, to protect effectively the data retained against any unauthorised access attempt and any unauthorised use, and so that an independent body is able to monitor the situation in a timely and efficient manner."[89]

As is well known, the stated purpose of the Directive was to harmonise the provisions concerning the obligations of telecommunications providers to retain data for the purpose of investigation, detection and prosecution of serious crime (the Directive, art. 1(1)), including terrorism (recitals 8–10). The Directive did not regulate access to the data (nor did it have the powers to) or its protection, where it relied on the general provisions of the Data Protection Directive[90] and the e-Privacy Directive. Inadequacy of the protective measures was part of the reason why the German Federal Constitutional Court found the German data retention transposition law invalid in its 2010 judgment. The standard of data security set by the Federal Constitutional Court is considerably higher than that which was required in the Data Protection Directive or even in the new General Data Protection Regulation.[91] The new law tries to implement this standard.

The requirement to store the data in Germany indicates an express distrust of the protection provided by the harmonised EU data protection rules. The government argues that if the data is stored in other EU countries, it could happen that "the foreign state shall have access to the data stored on its sovereign territory in accordance with its (national) law, something which, given recent experience, seems to be more than just a theoretical risk."[92]

Will distrust towards other Member States justify the restriction to the freedom to provide services? In *Ireland v European Parliament and the Council*,[93] the threshold to accept providers' data retention obligations as an internal market issue (European Community Treaty, art. 95, now TFEU, art. 114) was relatively low, even when the objective of the directive was the investigation, detection and prosecution of crime.[94] Respectively, is the weight of the internal-market objective equally as high when the freedom to provide data storage services is restricted on public policy and public security grounds? Would the CJEU accept distrust of other Member States as the justification?

DO MEMBER STATES COMPLY WITH THE CHARTER?

The above overview of Member State actions shows obvious differences in the reactions between different Member States. The reactions represent competing readings of what the Charter, as interpreted in *Digital Rights Ireland,* allows.[95] The permissive reading of the judgment sees the lack of proper safeguards as the reason why the court annulled the Directive. From this perspective, the observations which the court made in paras. 57–68 are a checklist of changes that would make the law proportionate, but is not an absolute list. Yet, "the basic undertone of the judgment nonetheless seems to be that some form of mandatory data retention in order to combat serious crime and terrorism might indeed be compatible with the EU Charter of Fundamental Rights."[96] According to the strict interpretation, the ruling, in practice, forbids any indiscriminate blanket data retention *per se* by requiring that the retained data must have a connection to serious crime and terrorism.[97] According to Husovec, para. 58 of the judgment presents an indispensable precondition because it is immediately followed by para. 59, which suggests how to proportionally limit the retention. It seems "very unlikely that the Court would make an exact suggestion of this kind, if it would not perceive this condition as a crucial one."[98] Taking the justification given for the Directive and the presumption of innocence in the Charter, art. 48, the looser the connection between the person and the unspecified, not-yet-actualised crime is, the more difficult it becomes to justify full-scale data collection. According to Boehm and Cole, "the Court clearly opposes the general indiscriminate mass collection of data."[99]

For the most part, political actors, such as governments and parliaments, seem to have favoured the permissive reading, while national courts have taken a stricter approach. How can these differences in approaches be explained? Several competing theories have been developed in the field of political studies to explain State compliance with EU law.[100]

The difficulty of measuring compliance with fundamental rights lies with their vagueness. Fundamental rights function as a ground of critique for governmental policies, but their actual effect on laws, such as the Directive, is dependent on the interpretation of the right in question. Some interpretations are provided by courts (in this case the CJEU), but when a judgment leaves room for uncertainty—like the *Digital Rights Ireland* judgment does—it would seem that governments tend to use that space to take the interpretation in the direction that best aligns with their policies. It also seems likely that ideological factors such as the composition of a coalition cabinet, or policy programs of different parties, have influence on how fundamental rights sensitive laws are implemented.

As shown above, two feasible readings of the *Digital Rights Ireland* judgment exist. This chapter does not aim to make any final conclusions about the right interpretation of the judgment. However, to test the theories, it is assumed in the following that the strict interpretation of the judgment is correct, because this seems to be more in line with the serious tone of the judgment. From this perspective, many Member States seem to be in apparent violation of the Charter of the Fundamental Rights. Two prominent approaches (enforcement and management based theories) from the compliance literature are tested to see if they can explain the Member State behaviour.

After this, a more theoretical and speculative approach is taken where conceptual analysis is used to explain the differences.

NONCOMPLIANCE AS POWER PLAY

Enforcement approaches of compliance studies assume that noncompliance with EU law is voluntary. States choose to violate legal norms because they are not willing to bear the costs of compliance. Therefore, sufficient sanctions increase compliance. Noncompliance can be prevented by monitoring and sanctioning—in the case of European Union, the monitoring is done by the European Commission and the sanctions are imposed by the Court of Justice of the European Union according to the TFEU, arts. 258 and 260. According to enforcement theories, the level of compliance is related to the amount of power a State holds (measured, *e.g.*, by its voting power).[101] In the enforcement stage, the more political or economic power a State has, the better it can resist the enforcement because it can afford to pay the reputational damages or financial penalties, while for smaller and less powerful States, a good reputation is of particular importance. In the decision-making stage, power means being able to better affect the EU legislation according to the State's preferences, which reduces the need for noncompliance.[102]

The governments of France, Ireland, Sweden and the U.K. were active in the early stages of the drafting of data retention legislation. Together, they proposed the Draft Framework Decision[103] that eventually lead to the adoption of the Directive. After *Digital Rights Ireland*, the U.K. seems to be unwilling to comply with the requirements of the judgment and has instead widened its surveillance legislation. Sweden is keeping its data retention law and refers to legal safeguards as a justification. France passed a surveillance law[104] in May 2015 that grants law enforcement and intelligence agencies access to communications metadata and other types of surveillance without court authorisation. Telecommunications metadata will be retained for up to 4 years.[105] The law was reviewed and accepted for the most part

by the Constitutional Committee.[106] States like Denmark, Finland, the Netherlands and others still adhere to the permissive interpretation and have not changed their legislation.

It seems fair to ask if these Member States are actually acting in good faith because the judgment did not significantly alter their views of what is permissible. In some Member States (such as the U.K., Finland, Denmark and Sweden), government reactions and new data retention laws do not substantially differ from the annulled laws. Nevertheless, these Member States claim they are now in compliance.

It is possible that the States actually agree that the judgment sets far-reaching limits on surveillance laws, but are unwilling to accept these limitations to their powers. The strict interpretation is based on a prohibition of mass surveillance, while the permissive interpretation benefits from the vagueness of the judgment. EU legislation is often loosely worded and ambiguous as a result of the need to accommodate differences between the Member States and the interests of the multitude of actors involved in the process.[107] It is precisely this vagueness that allows the governments to use the proportionality argument: That blanket retention is not forbidden as such and it is legal if sufficient conditions regarding limitations and legal safeguards are in place. The CJEU leaves open the conditions that are absolutely required for proportionality: Is it all conditions listed in *Digital Rights Ireland*, paras. 57–67, or just some of them? Some Member States have re-implemented data retention after the judgment with only minor changes—shorter retention periods, fewer data types stored *etc.*—but still keeping the main idea of blanket retention. Vagueness of the judgment leaves these Member States room to argue their implementation is proportionate because it addresses some of the worries the court listed.

The Member States that were strong proponents of data retention in the beginning retain this position even after the Directive has been repealed. Their goals were accomplished in part by the passing of the Directive. States are now reluctant to follow an interpretation that would require them to stop data retention. This is the strategy of "opposition through the backdoor".[108]

Open refusal to implement a directive, even after the court has reviewed its legality, is not an unknown event in EU history.[109] Although the U.K. in general has a good compliance record,[110] here it seems to be counting on the fact that is has enough economic and political power to get away with the infringement.

MANAGEMENT APPROACHES: INVOLUNTARY NONCOMPLIANCE

Management approaches assume that noncompliance is involuntary. It is assumed that noncompliance results from the absence of required preconditions. According to the literature,[111] three causes of involuntary compliance are:

(1) Insufficient State capacities,
(2) Ambiguous definitions of norms, and
(3) Inadequate timetables within which compliance has to be achieved.

State capacities are defined as a State's ability to act—that is, the sum of its legal authority and financial, military and human resources. Even if a State has adequate resources, its administration may have difficulties in pooling and coordinating them, either because of institutional structures or because of an inefficient bureaucracy.

In the case of Member States that have not taken any legislative actions after the judgment (for example Sweden, the Czech Republic and Portugal), it could be speculated whether administrative difficulties (lack of resources, inefficient bureaucracy and similar) are the reason why these States did not change their laws to strengthen the protection of privacy, but this explanation seems unlikely. However, in the case of States that have intentionally taken actions that affirm previous data retention regime, or even go further in the data collection, noncompliance with the judgment obviously cannot be explained by a lack of resources.

Factors related to the constitutional design of a State, such as the existence of a constitutional court, can influence the implementation of EU directives and the Charter. No evidence exists to show that that non-compliance with the judgment would be a consequence of such structures. The contrary, however, may be true—past decisions of the national constitutional courts may have affected government reactions. This seems likely in the case of Germany, where the government proposed a very moderate new version of the data retention regime. In the light of the Constitutional Court's decision in 2010, a heavier and more invasive data retention law probably would not be accepted by the Constitutional Court.

SECURITY BIAS

If we assume there is a genuine disagreement about the limits that the *Digital Rights Ireland* judgment sets, we should look at institutional and cultural factors as an explanation for the obvious difference in interpretations. This

would include analysis of the roles of constitutional courts and legislators as protectors of the constitution in the Member States. Do the courts take fundamental and human rights more seriously than the governments and why?

The constitutional courts in the continental Member States have interpreted the requirements in *Digital Rights Ireland* strictly and most of them found the national laws as being in conflict with the national constitution (an exception being the Polish Constitutional Tribunal). This may indicate the courts' self-understanding as protectors of the national, and possibly also the European, constitution (although this enthusiasm was not shared by the U.K. Court of Appeal, which preferred a narrower interpretation of the CJEU's judgment). In the actions of the Member State governments, fundamental rights do not seem to have similar weight. What explains this?

In the fundamental rights theory,[112] a collision of a fundamental right with a collective good, such as national security, is usually seen as a situation that requires "balancing" and "proportionality" to define the right legal outcome. Such "balancing exercises" are required when laws are applied by an authority or a court because fundamental rights provisions are vague and open to interpretation.[113]

I argue that the narrow reading of the judgment, followed by, *e.g.*, the U.K., is based upon a presupposition that I call "security bias". A central feature of the security-biased interpretation is that its analysis of security risks is vague and indefinite, yet still it represents risks as urgent and severe. For example, the then Prime Minister, Mr. David Cameron, presented a serious view while defending the new British emergency legislation after the *Digital Rights Ireland* judgment: "So failure to act now would fundamentally undermine our capability to counter a range of threats to the safety of our citizens, and I will not stand by and let that happen."[114] The then Deputy Prime Minister's warning was more direct: "[C]ommunications data and lawful intercept are now amongst the most useful tools available to us to prevent violence and bloodshed on Britain's streets."[115]

Mr Cameron's list of possible threats ranged from paedophiles to organised terrorist groups:

> "Now, we face real and credible threats to our security from serious organised crime, from the activity of paedophiles, from the collapse of Syria, the growth of ISIS in Iraq and Al Shabaab in East Africa. And I'm simply not prepared to be a Prime Minister who has to address the people after a terrorist incident and explain that I could have done more to prevent it."[116]

The argument was straightforward: If communications could not be intercepted, safety would be seriously endangered.

Another element of the security bias is the way privacy and security are conceptualised. The argument is presented in a way that suggests that metadata surveillance is about giving up a small amount of privacy (only metadata, not content) in exchange for great potential national gain. According to this argument, the information collected is not particularly sensitive, only computers and selected officials will see it, and an honest, law-abiding person should have no concerns because they have "nothing to hide." Therefore, the value of the right to privacy would be low in this balancing exercise. On the other side of the scale, national security is assigned very high value. Security risks are described only in general terms (see Mr. Cameron's references to terrorist groups above) but potential risks are depicted as "bloodshed on Britain's streets". When arranged like this, the argument is convincing—the security interest should prevail.[117]

Of course, this isn't the only possible understanding of the equation. In the security-biased view, privacy is understood narrowly. The argument would prevail only if privacy was primarily used to hide things which ought to be in full view.[118] However, privacy cannot be reduced to only concealing of facts, or "right to be left alone", or "intimacy". Privacy is a set of rights responding to a large set of specific problems. Harm caused by revealing information is only one of the problems which a right to privacy is trying to prevent.

The problem is not only about the collection of the data which itself may be non-sensitive. As the CJEU argued, by aggregating communications data and other data collected from other sources, the government is able to construct personal profiles that reveal sensitive facts about the person, even if the original data was trivial and non-sensitive. Profiles may be used to predict our future actions and to categorise us (including the categorisation of citizens as a "risk"). The person affected may not even know about the existence of such profile, nor have the ability to check its accuracy or have errors corrected. What makes this a problem is not the person's inability to hide facts from others but their lack of control in how data concerning them is used. Use of surveillance data thus becomes a problem of power imbalance.[119] We should also recall that large-scale data collection presents risks because that data can be obtained and used by persons other than the authorities originally empowered to collect it. Recent revelations about hacking in government data centres and, indeed, the revelations about surveillance from within, underline this point.

The problem with the "nothing to hide" argument is that it only takes into account one of the problems to which the right to privacy tries to respond, namely the need to control personal facts. This is a completely different problem than the power imbalance problem. "Hiding facts about oneself" conceptualises privacy as an individual right. If one person's right is balanced against the general security interest, security is likely to outweigh

the individual right. This, however, is an inadequate balancing. Properly done, the balancing will include all the components of privacy, including the social components, such as the need for balance of informational power. The outcome of such balancing exercise would be less obvious.

HAS THE CHARTER FAILED TO PROTECT PRIVACY?

Some theoretical accounts of the reasons why not all Member States follow the stricter, fundamental-rights friendly interpretation were given above. It seems likely that either some States resist the strict interpretation intentionally for political reasons. Another explanation is the security bias: that those Member States have adopted an inadequate conception of privacy that leads to a biased balancing.

What are the consequences for the right to privacy and the Charter of Fundamental rights in general? It will depend on how the European Commission reacts to the situation. Monitoring the compliance of EU legislation, including the Treaties, is a duty of the European Commission. If the Commission suspects non-compliance, it may start an infringement procedure in accordance with the TFEU, art. 258. The review of compliance with EU fundamental rights has been high on the political agenda and has resulted in the addition of a clause on the suspension of Treaty rights (Treaty of the European Union, art. 7). So far, the Commission has announced it will not propose any new data retention directive and will "continue monitoring legislative development at national level".[120] The Commission's enforcement activities are of particular importance for the maintenance of the rule of law in the EU, especially taking into account the recent negative developments in Member States such as Hungary and Poland.[121]

The Charter of Fundamental Rights promises strong fundamental rights protection. Yet, the CJEU's declaration of the invalidity of the Directive did not have all of the expected consequences. Some Member States have enacted new retention laws similar to the annulled directive. Others have remained passive, keeping the old laws in place. Protection of privacy in the field of electronic communications has not been harmonised, as promised by the Charter. The judicial process will go on as the CJEU will this time answer the more direct questions on the legality of a general blanket retention.[122] How the Commission proceeds with its monitoring is in itself a political decision that will affect the efficiency of the Charter. Should the Commission fail to take action, it might be fair to say the Charter has failed to protect the right to privacy.

[1] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 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 [2006] OJ L105/54.

[2] For a general overview of the fundamental rights impact of data retention, see Patrick Breyer, "Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR" (2005) 11 (3) European Law Journal 365.

[3] The Directive, art. 6.

[4] European Data Protection Supervisor, "Opinion of the European Data Protection Supervisor on the proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC (COM(2005) 438 final)" (29 November 2005) [2005] OJ C298/01.

[5] Article 29 Working Party, "Opinion 4/2005 on the Proposal for a Directive of the European Parliament and of the Council on the Retention of Data Processed in Connection with the Provision of Public Electronic Communication Services and Amending Directive 2002/58/EC (COM(2005)438 final of 21.09.2005)" (2005).

[6] For an overview of the cases, see Eleni Kosta, "The Way to Luxemburg: National Court Decisions on the Compatibility of the Data Retention Directive with the Rights to Privacy and Data Protection" (2013) 10 (3) SCRIPTed 339; Niklas Vainio & Samuli Miettinen, "Telecommunications Data Retention after Digital Rights Ireland: Legislative and Judicial Reactions in the Member States" (2015) 23 (3) International Journal of Law and Information Technology 290.

[7] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland v Minister for Communications, Marine and Natural Resources* (Grand Chamber, 8 April 2014). Available online at <http://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang=EN>, accessed 20 October 2016.

[8] Elements of this paper are based on Vainio & Miettinen (n 6).

[9] The Directive, recital 13, art. 1(2) and art. 5(2).

[10] For a detailed analysis, see Vainio & Miettinen (n 6) 297–299.

[11] The table is based on the Council of the European Union, Document 14246/15 (24 November 2015) with updates by the author. Information on some Member States is limited so inaccuracies are possible.

[12] With regard to some Member States, access to information on the status of national data retention laws is limited by a language barrier, but it is the author's understanding that the chosen Member States represent the range of different reactions appropriately.

[13] Decision G 47/2012-49, *Seitlinger*, 27 June 2014. See the press release of the court available online at <https://www.vfgh.gv.at/cms/vfgh-site/attachments/1/5/8/CH0006/CMS1409900579500/press_releasedataretention.pdf>, accessed 20 October 2016.

[14] Case number PL. ÚS 10/2014. See EISi, "Full version of the decision invalidating the data retention in Slovakia now available, the legislator has 6 months to come up with compliant provisions" (*European Information Society Institute*, 2015) <http://www.eisionline.org/index.php/en/projekty-m-2/ochrana-sukromia/120-data-retention-full-version>, accessed 20 October 2016.

[15] Martin Husovec, "Slovak Constitutional Court Annuls National Data Retention Provisions" (2015) 1 (3) European Data Protection Law Review 227.

[16] *ibid*. 228.

[17] EISi (n 14).

[18] Husovec (n 15) 228.

[19] *ibid*. 229.

[20] "Data retention across the EU" (*European Union Agency for Fundamental Rights*) <http://fra.europa.eu/en/theme/information-society-privacy-and-data-protection/data-retention>, accessed 20 October 2016.

[21] Judgment of the Constitutional Court of Slovenia on 3 July 2014, U-I-65/13-19.

[22] Information Commissioner of Slovenia, "Slovenian Constitutional Court holds data retention unconstitutional, orders deletion of data" (11 July 2014) <https://www.ip-rs.si/en/news/slovenian-constitutional-court-holds-data-retention-unconstitutional-orders-deletion-of-data-1256/>, accessed 20 October 2016.

[23] Decision No. 1258 of 8 October 2009. Unofficial translation by Bogdan Manolea & Anca Argesiu available online at <http://www.legi-internet.ro/fileadmin/editor_folder/pdf/decision-constitutional-court-romania-data-retention.pdf>, accessed. 30 October 2016.

[24] EDRi, "Romanian Parliament adopts the data retention law. Again." (*European Digital Rights*, 23 May 2012) <http://edri.org/edrigramnumber10-10romanian-parliament-adopts-data-retention-law-again/>, accessed 20 October 2016.

[25] See the press release of the court, in Romanian: <http://www.ccr.ro/noutati/COMUNICAT-DE-PRES-99>, accessed 2 June 2015; Bogdan Manolea, "Romania: The aftermath of the second CCR data retention ruling" (*European Digital Rights*, 8 October 2014) <https://edri.org/romania-aftermath-of-second-ccr-data-retention-ruling/>, accessed 20 October 2016.

[26] "Data Retention Legislation Comes into Force in Bulgaria" (*Novinite*, 10 May 2010) <http://www.novinite.com/articles/116025/Data+Retention+Legislation+Comes+into+Force+in+Bulgaria>, accessed 20 October 2016.

[27] Evgeniya Scherer, "New Developments of the Legal Framework on the Retention of Data in Bulgaria" (2015) 1 (3) European Data Protection Law Review 219, 220–221.

[28] *ibid*. 221.

[29] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L201/37.

[30] Scherer (n 27), 220–221.

[31] Letter titled "Reactie van het kabinet naar aanleiding van de ongeldigverklaring van de richtlijn dataretentie" (17 November 2014); translation by Matthijs R. Koot available online at <https://blog.cyberwar.nl/2014/11/dutch-govt-response-to-ecjs-april-2014-ruling-on-the-eu-data-retention-directive/>, accessed 20 October 2016.

[32] *ibid*.

[33] Judgment of the District Court of The Hague, 11 March 2015 (ECLI:NL:RBDHA:2015:2498). Description of the case based on the unofficial translation by Anna Berlee <http://theiii.org/documents/DutchDataRetentionRulinginEnglish.pdf>, accessed 20 October 2016.

[34] Rejo Zenger, "Bewaarplicht van tafel – voor nu" (*Bits of Freedom*, 11 March 2015) <https://www.bof.nl/2015/03/11/bewaarplicht-van-tafel-voor-nu/>, accessed 20 October 2016.

[35] Constitutional Court of Belgium, judgment 84/2015, para. B.11.

[36] Laurens Naudts, "Belgian Constitutional Court Nullifies Belgian Data Retention Law" (2015) 1 (3) European Data Protection Law Review 208, 210–211.

[37] *ibid.* 211.

[38] Prime Minister's Office, "PM and Deputy PM speech on emergency security legislation" (*Gov.uk*, 11 July 2014) <https://www.gov.uk/government/speeches/pm-and-deputy-pm-speech-on-emergency-security-legislation>, accessed 20 October 2016.

[39] U.K. Data Retention and Investigatory Powers Act 2014.

[40] Graham Smith, "Dissecting DRIP - the emergency Data Retention and Investigatory Powers Bill" (*Cyberleagle*, 12 July 2014) <http://cyberleagle.blogspot.co.uk/2014/07/dissecting-emergency-data-retention-and.html>, accessed 20 October 2016.

[41] Liberty & others, "Liberty, Privacy International, Open Rights Group, Big Brother Watch, Article 19 and English PEN briefing on the fast-track Data Retention and Investigatory Powers Bill" <https://www.openrightsgroup.org/assets/files/pdfs/reports/DRIP_joint_briefing.pdf> para. 12, accessed 20 October 2016.

[42] "Data Retention and Investigatory Powers Bill: Government Note on the European Court of Justice Judgment" <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/331106/DRIPgovernmentNoteECJjudgment.pdf>, accessed 20 October 2016.

[43] Smith (n 40); Liberty (n 41).

[44] Liberty (n 41) para. 30.

[45] *Davis v Secretary of State for the Home Department* [2016] 1 CMLR 13; [2015] EWHC 2092 (Admin).

[46] *ibid*. [6]–[7].

[47] *ibid.* [83].

[48] *ibid*. [89].

[49] *Kennedy v U.K.* (2011) 52 EHRR 4.

[50] *Davis* [73].

[51] Lorna Woords, "High Court Strikes Down Data Retention Laws in Ruling on DRIPA" (2015) 1 (3) European Data Protection Law Review 236, 237.

[52] *Davis* [91].

[53] *ibid*. [122].

[54] [2016] 1 CMLR 48; [2015] EWCA Civ 1185, [80].

[55] *ibid*.

[56] *ibid*. [103].

[57] *ibid.* [115].

[58] *ibid.* [118]. At the CJEU, this case is numbered titled C-698/15 *Secretary of State for Home Department v Watson*.

[59] Investigatory Powers Bill, as amended in committee (12 September 2016), 78(9). See explanation to the clause, *Investigatory Powers Bill: Explanatory Notes*, available online at <http://www.publications.parliament.uk/pa/bills/lbill/2016-2017/0040/17040en.pdf> 38, accessed 21 October 2016.

[60] Liam Tung, "Four of Sweden's telcos stop storing customer data after EU retention directive overthrown" (*ZDNet*, 11 April 2014) <http://www.zdnet.com/four-of-swedens-telcos-stop-storing-customer-data-after-eu-retention-directive-overthrown-7000028341/>, accessed 21 October 2016; Karolina Schützer, "Teleoperatörer stoppar datalagring" (*SVT*, 8 May 2014) <http://www.svt.se/nyheter/teleoperatorer-gar-mot-svensk-lag>, accessed 21 October 2016.

[61] Post- och telestyrelsen, "PTS kommer inte i nuläget att vidta åtgärder utifrån datalagringsreglerna" (10 April 2014) <http://www.pts.se/sv/Nyheter/Telefoni/2014/PTS-kommer-inte-i-nulaget-att-vidta-atgarder-utifran-datalagringsreglerna/>, accessed 21 October 2016.

[62] Memorandum Ds 2014:23 (Datalagring, EU-rätten och svensk rätt) 13 June 2014. Available online at < http://www.regeringen.se/rattsdokument/departementsserien-och-promemorior/2014/06/ds-201423/>, accessed 30 October 2016.

[63] PTS decision of 27 June 2014 (Dnr 14-4175). Available online at <http://www.pts.se/upload/Beslut/Internet/2014/14-4175-forelaggande-lagring-Tele2.pdf>, accessed 21 October 2016.

64 Case C-203/15 *Tele2 Sverige AB v Post-och telestyrelsen*.

65 Pam Storr, "Blanket Storage of Communications Data - Proportional or Not? Sweden Asks CJEU for Clarification on Data Retention" (2015) 1 (3) European Data Protection Law Review 230, 233.

66 Committee statement PeVL 18/2014 vp.

67 Committee report LiVM 10/2014 vp.

68 Ministry of Defence, "Suomalaisen tiedustelulainsäädännön suuntaviivoja. Tiedonhankintalakityöryhmän mietintö" (2015). Available online at <http://www.defmin.fi/files/3016/Suomalaisen_tiedustelulainsaadannon_suuntaviivoja.pdf>, accessed 21 October 2016.

69 "Notat om betydningen af EU-Domstolens dom af 8. april 2014 i de forenede sager C-293/12 og C-594/12 (om logningsdirektivet) for de danske logningsregler" (2 June 2014).

70 Henry Järvinen, "Denmark: Data retention is here to stay despite the CJEU ruling" (*European Digital Rights*, 4 June 2014) <https://edri.org/denmark-data-retention-stay-despite-cjeu-ruling/>, accessed 21 October 2016.

71 "Notat om betydningen af EU-Domstolens dom af 8. april 2014 i de forenede sager C-293/12 og C-594/12 (om logningsdirektivet) for de danske logningsregler" (n 69) 29–30.

72 *ibid*. 22. On the usefulness of session logging, see Jesper Lund, "Danish government wants to postpone the evaluation of the data retention law for the third time" (*IT-Politisk Forening*, 12 February 2013) <https://itpol.dk/notater/Danish-data-retention-evaluation-Feb13>, accessed 21 October 2016.

73 Anneli Albi, "Supremacy of EC Law in the New Member States; Bringing parliaments into the Equation of 'Co-operative Constitutionalism'" (2007) 3 (1) European Constitutional Law Review 25, 62.

74 Katarzyna Szymielewicz, "Blanket data retention in Poland: The issue and the fight" (*Panoptykon Foundation*). Available online at <http://www.ohchr.org/Documents/Issues/Privacy/PanoptykonFoundation.pdf>, accessed 21 October 2016.

75 European Commission, "Evaluation report on the Data Retention Directive (Directive 2006/24/EC)" COM (2011) 225 final (Brussels, 2011) 40.

76 Remigiusz Rosicki, "Surveillance and Data Retention in Poland" (2014) 1 (5) Public Policy and Economic Development 63, 65.

77 Kosta (n 6).

78 "Data retention across the EU" (n 20).

79 "Bulgaria scrambles to amend scrapped data retention provisions" (*The Sofia Globe*, 26 March 2015) <http://sofiaglobe.com/2015/03/26/bulgaria-scrambles-to-amend-scrapped-data-retention-provisions/>, accessed 21 October 2016.

80 German Federal Constitutional Court judgment of 2 March 2010, 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08.

81 Sebastian Schweda, "Parliament Adopts New Data Retention Law" (2015) 1 (3) European Data Protection Law Review 223, 225.

82 EDRi, "German Federal Constitutional Court rejects data retention law" (*European Digital Rights*, 10 March 2010) <https://edri.org/edrigramnumber8-5german-decision-data-retention-unconstitutional/>, accessed 21 October 2016.

83 European Commission infringement procedure 20112091.

84 "Deutschlands Zukunft gestalten. Koalitionsvertrag zwischen CDU, CSU und SPD. 18. Legislaturperiode" <http://www.bundesregierung.de/Content/DE/_Anlagen/2013/2013-12-17-koalitionsvertrag.pdf?__blob=publicationFile&v=2> 147, accessed 21 October 2016.

[85] "Entwurf eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten" Drucksache 18/5088 (9 June 2015). Available online at <http://dip.bundestag.de/btd/18/050/1805088.pdf>, accessed 21 October 2016.

[86] Schweda (n 81) 225–226.

[87] *ibid*. 226.

[88] Jakob May, "Weitere Verfassungsbeschwerde gegen Vorratsdatenspeicherung eingereicht" (*Netzpolitik*, 27 January 2016) <https://netzpolitik.org/2016/weitere-verfassungsbeschwerde-gegen-vorratsdatenspeicherung-eingereicht/>, accessed 21 October 2016.

[89] "Governmental draft of the Federal Ministry of Justice and Consumer Protection Draft Act introducing a storage obligation and a maximum retention period for traffic data" (English translation) 45. Available online at <http://ec.europa.eu/growth/tools-databases/tris/de/index.cfm/search/?trisaction=search.detail&year=2015&num=288&dLang=EN>, accessed 21 October 2016.

[90] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31.

[91] Regulation (EU) 2016/679 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 and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.

[92] "Governmental draft of the Federal Ministry of Justice and Consumer Protection Draft Act introducing a storage obligation and a maximum retention period for traffic data" (n 89) 45.

[93] Case C-301/06 *Ireland v European Parliament and the Council* [2009] ECR I-00593.

[94] *ibid.* paras. 58–59.

[95] On the permissive/strict distinction, see Vainio & Miettinen (n 6), 299–300.

[96] SURVEILLE Project, "SURVEILLE Paper Assessing Surveillance in the Context of Preventing a Terrorist Act" (29 May 2014) <http://justsecurity.org/wp-content/uploads/2014/10/SURVEILLE-Paper-on-a-Terrorism-Prevention.pdf> 43, accessed 21 October 2016.

[97] Steve Peers, "The data retention judgment: The CJEU prohibits mass surveillance" (*EU Law Analysis*, 8 April 2014) <http://eulawanalysis.blogspot.fi/2014/04/the-data-retention-judgment-cjeu.html>, accessed 21 October 2016.

[98] Martin Husovec, "First European Constitutional Court Suspends Data Retention after the Decision of the Court of Justice of EU" (*The Center for Internet and Society*, 28 April 2014) <http://cyberlaw.stanford.edu/blog/2014/04/first-european-constitutional-court-suspends-data-retention-after-decision-court>, accessed 21 October 2016.

[99] Franziska Boehm & Mark Cole, "Data Retention after the Judgement of the Court of Justice of the European Union" (2014) <http://www.greens-efa.eu/fileadmin/dam/Documents/Studies/Data/Boehm_Cole_-_Data_Retention_Study_-_June_2014.pdf> 36, accessed 21 October 2016.

[100] See, *e.g.*, Risto Lampinen & Petri Uusikylä, "Implementation Deficit – Why Member States do not Comply with EU directives?" (1998) 21 (3) Scandinavian Political Studies 231; Tanja Börzel, Tobias Hofmann, Diana Panke & Carina Sprungk, "Obstinate and Inefficient: Why Member States Do Not Comply With European Law" (2010) 43 (11) Comparative Political Studies 1363; Diana Panke, "The European Court of Justice as an agent of Europeanization? Restoring compliance with EU law" (2007) 14 (6) Journal of European Public Policy 847.

[101] Tanja Börzel, Tobias Hofmann, Diana Panke & Carina Sprungk (n 100) 1375.

[102] *ibid*. 1367–1368.

[103] The French Republic, Ireland, the Kingdom of Sweden and the U.K., "Draft Framework Decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism" Council Document 8958/04 (Brussels, 28 April 2004).

[104] Law no 2015-912 of 24 July 2015.

[105] Angelique Chrisafis, "France passes new surveillance law in wake of Charlie Hebdo attack" (*The Guardian*, 5 May 2015) <http://www.theguardian.com/world/2015/may/05/france-passes-new-surveillance-law-in-wake-of-charlie-hebdo-attack>, accessed 21 October 2016; Bénédicte Dambrine, "The State of French Surveillance Law" (*Future of Privacy Forum*, 22 December 2015) 7. Available online at <https://fpf.org/wp-content/uploads/2015/12/Surveillance-law-in-France_Dec2015.pdf>, accessed 21 October 2016.

[106] Décision n 2015-713 DC du 23 juillet 2015.

[107] Gerda Falkner, Miriam Hartlapp, Simone Leiber & Oliver Treib, "Non-Compliance with EU Directives in the Member States: Opposition through the Backdoor?" (2004) 27 (3) West European Politics 452, 463.

[108] *ibid*. 453.

[109] *ibid*. 457–458; Case C-84/94 *U.K. v Council of the European Union* [1996] ECR I-05755.

[110] Tanja Börzel, Tobias Hofmann, Diana Panke & Carina Sprungk (n 100) 1381–1382.

[111] See *ibid*. 1369.

[112] See, *e.g.*, Robert Alexy, *A Theory of Constitutional Rights* (Oxford University Press 2002).

[113] For a critique of balancing and proportionality arguments, see Grégoire Webber, "Proportionality, Balancing, and the Cult of Constitutional Rights Scholarship" (2010) 23 (1) Canadian Journal of Law and Jurisprudence 179.

[114] Prime Minister's Office (n 38).

[115] *ibid*.

[116] *ibid*.

[117] Daniel Solove, "'I've Got Nothing to Hide' and Other Misunderstandings of Privacy" (2007) 44 San Diego Law Review 745, 752–753.

[118] *ibid*. 764.

[119] *ibid*. 764–766.

[120] Diego Naranjo, "European Commission will 'monitor' existing EU data retention laws" (*European Digital Rights*, 29 July 2015) <https://edri.org/european-commission-will-monitor-existing-eu-data-retention-laws/>, accessed 21 October 2016.

[121] See, *e.g.*, the Opinions of the Venice Commission on Hungary, CDL-AD(2013)012, and Poland, CDL-AD(2016)001.

[122] On 19 July 2016, Advocate General Saugmandsgaard Øe published his Opinion (ECLI:EU:C:2016:572) regarding the *Tele2* and *Watson* references. In his reading, the *Digital Rights Ireland* judgment requires that data retention obligations must be accompanied by all the safeguards described by the CJEU in paras. 60–68 of the judgment. The Opinion suggests that blanket data retention may be legal in principle, but the required conditions are so strict that this may remain only a theoretical possibility. The Opinion is available online at <http://curia.europa.eu/juris/document/document.jsf?docid=181841&doclang=EN>, accessed 21 October 2016. See also Lorna Woods, "Analysing the Advocate General's opinion on data retention and EU law" (*Information Law & Policy Centre*, 27 July 2016) <https://infolawcentre.blogs.sas.ac.uk/2016/07/27/analysing-the-advocate-generals-opinion-on-data-retention-and-eu-law/>, accessed 21 October 2016. After this Opinion, a Spanish court has submitted yet another request for a preliminary ruling regarding the severity of a suspected crime that is used as the grounds for access to the retained data in C-207/16 *Fiscal*.