PRIVACY INTERNATIONAL

A Concerning State of Play for the Right to Privacy in Europe

National Data Retention Laws since the CJEU's Tele-2/Watson Judgment

September 2017

NATIONAL DATA RETENTION LAWS SINCE THE CJEU'S TELE-2/WATSON JUDGMENT

A Concerning State of Play for the Right to Privacy in Europe

September 2017

PRIVACY INTERNATIONAL

www.privacyinternational.org

Table of Contents

Introduction	4
Data Retention Practices: Legal and Practical Issues	6
Data Retention in the European Union	7
Data Retention under European and International Human Rights Law	10
Member State Laws post Tele-2/Watson: the current State of Affairs	12
Conclusions and Recommendations	14
National Data Retention Policies pre- and post Tele- 2/Watson (7 July 2017)	15

Introduction

The practice of mandating the retention of communications data (or metadata) by Telecommunications companies, as prescribed by the laws of most European Union Member States, raises significant privacy, transparency and security concerns. Telecommunications companies and service providers are required by law to store large amounts of personal data on an ongoing basis for later access by Government agencies and local authorities, but such storage and access is often indiscriminate and fails to guarantee sufficient safeguards from abuse. As the data generated by smart phones increases, the data Governments' demand is retained, is or is likely to go far beyond that necessarily required for business purposes.

In two judgments, the *Digital Rights Ireland* case (2014)[1] and the more recent *Tele-2/Watson* decision (2016),[2] the Court of Justice of the European Union (CJEU) reaffirmed the requirement that all data retention regimes must comply with the principles of legality, necessity, and proportionality. Unfortunately, this basic standard laid down by the CJEU is not adhered to by most EU member states, despite their legal obligation to comply with the Court's jurisprudence. National data retention regimes are often outdated and lack clarity. In some states these regimes are the subject of prolong challenges before national Courts, which further enhance uncertainty. Telecommunications operators like Tele2 and Telia in Sweden[3] or Spacenet[4] in Germany are clearly expressing discomfort with the current state of affairs.

This report is an attempt to shed light as to the current state of affairs in data retention regulation across the EU post the Tele-2/Watson judgment. Privacy International has consulted with digital rights NGOs and industry from across the European Union to survey 21 national jurisdictions (Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, France, Germany, Hungary, Ireland, Italy, Luxembourg, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, and the United Kingdom). Tracking legislation and jurisprudence across different jurisdictions is often a challenge: while this report aims to be a comprehensive survey of data retention regimes in the EU to date, Privacy International would be grateful to receive any additional information, updates and clarification.

The Report concludes that all EU member States surveyed are not in compliance with the Tele-2/Watson decision. The report further notes that in many EU member States

1 Digital Rights Ireland Ltd v. Minister of Communications, Marine and Natural Resources et al. (C-293/12); Kärntner Landesregierung and others (C-594/12), Joined Cases, Court of Justice of the European Union, Grand Chamber, Judgment (8 April 2014).

2 Tele2 Sverige AB v. Post- Och telestyrelsen (C-203/15); Secretary of State for the Home Department v. Tom Watson et. al. (C-698/16), Joined Cases, Court of Justice of the European Union, Grand Chamber, Judgment (21 December 2016). Privacy International was an intervener in that case.

3 See e.g., http://betterbusiness.tele2.se/2016/12/datalagring-kan-hos-tele2/ (Tele-2, 27 December 2016); http://press.telia.se/news/datalagringsfraagan-vi-behoever-en-lagstiftning-som-tillgodoser-saavael-behovet-av-brottsbekaempning-som-behovet-av-integritet-210198 (Telia, 30 December 2016).

4 See e.g., https://www.twobirds.com/en/news/articles/2017/germany/german-traffic-data-retention-law-considered-invalid (26 June 2017).

legislation is not even in conformity with the earlier *Digital Rights Ireland* decision. Based on Privacy International's findings and 8-months into the *Tele-2/Watson* ruling, Privacy International makes the following main recommendations:

All EU member States should review their legislation and, if necessary, amend it to comply with European standards, including the CJEU jurisprudence;

Telecommunications and other companies subject to data retention obligations should challenge existing data retention legislation which are not compliant with European standards, including the CJEU jurisprudence;

The European Commission should provide guidance on reviewing national data retention laws to ensure its conformity with fundamental rights, as interpreted by the CJEU.

Data Retention Practices: Legal and Practical Issues

The practice of data retention involves the gathering and storing of communications data for extended periods for the purpose of future access. Metadata tells the story about your data and answers the who, when, what, and how of a specific communication. Data collected will likely cover a mixture of personally identifiable and non-identifiable information, including traffic data (data about how a communication was transmitted including source, destination, means of transmission, time and location of transmission), subscriber data (data identifying subscribers as provided to the communications service provider) and data specific to the use of the communications service in question (time of use, billing information, amount of data downloaded, redirection services).[5] Data retention serves multiple uses, some of which are commercial and others are not. Retention can similarly be voluntary, for instance where the data is kept by a company for its internal uses, or it can be mandated by law for potential access by third parties, in particular by governmental agencies.

The potential harms associated with data retention and access are significant. In a context where the gathering and exploitation of data by private companies becomes increasingly privacy intrusive and widespread, data retention poses serious risks to individual privacy and data security. The data opens the door for governments and third parties to make intimate inferences about individuals, to engage in profiling and to otherwise intrude on people's private lives.[6] If the information is not properly protected there is the potential of unauthorised access to troves of information by third parties, including cyber-criminals.

The laws in most countries treat separately the question of the retention of data and the access to it for law enforcement or intelligence purposes. The two issues are, however, closely intertwined. Poorly drafted data retention legislation increases the chances of indiscriminate collection and access that risks abuses of power. For example, the absence of limitations on retention (e.g. the absence of proper deletion mechanisms for irrelevant information or of proportionate retention periods) increases the likelihood for security beaches and for unauthorised access. Similarly, broad, vague or ill-defined rules on governmental access to retained data can lead to unlawful surveillance, a rise in collateral data (the incidental access to information of individuals who are not related to the subject of the investigation), misuse and other abuses of data protection standards (e.g. sharing of personal data).

Consequently, safeguards must be put in place to ensure that the interference with fundamental rights is minimised at both the retention and the access stages. The

[5] See e.g. David Anderson Q.C., A Question of Trust: Report of the Investigatory Powers Review (June 2015), para. 6.6, available at https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Print-Version.pdf.

[6] As noted by the CJEU in the Tele2/Watson decision, retained data allows for the drawing of "very precise conclusions… concerning the private lives of the persons whose data has been retained... In particular, that data provides the means… of establishing a profile of the individuals concerned" (see supra note 2, at para. 99).

human rights standards on data retention developed by the CJEU, the European Court of Human Rights (to which all EU Member States are also bound, by their being parties to the European Convention of Human Rights) and the UN human rights mechanisms, seek to ensure that the individuals whose data is being retained are adequately empowered to protect themselves against all of these associated risks.

Data Retention in the European Union

In the EU, privacy is afforded protection under the EU Charter of Fundamental Rights at Article 7 (respect for private and family life), and Article 8 (protection of personal data) as well as under the limitations and guarantees of Article 52.[7]

The e-Privacy Directive (2002/58/EC), Article 15, provides that

> "Member States may … adopt legislative measures providing for the retention of data for a limited period [where data retention constitutes] a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system [and provided the data retention measures are] in accordance with the general principles of Community law".[8]

A few years after the e-Privacy Directive, another Directive, No. 2006/24,[9] was adopted to ensure harmonisation between Member States' data retention regimes and to impose an obligation on the providers of publicly available electronic communications services or of public communications networks to retain certain data generated or processed by them. Article 3 of the Directive asked Member States to adopt measures to ensure that the types of data listed in Article 5 (metadata on the sources, destination, duration of communications, etc.) be retained for a period of between 6 months and 2 years, as specified in Article 6. Article 4 of that Directive was very sparse on details and afforded Member States a large margin of discretion as to what constituted lawful access.

In its judgment in Digital Rights Ireland of April 2014, the CJEU held Directive 2006/24 to be invalid as a disproportionate exercise of the EU legislature's powers in breach of Articles 7, 8 and 52(1) of the EU Charter of Fundamental Rights.[10] In that case the CJEU

7 Note further that the European Convention on Human Rights, to which the EU is a member in its own right, also recognises the right to a private and family life under Article 8 ECHR.

8 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), OJ L 201, p. 37–47, Article 15(1) (31 July 2002).

9 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, OJ L 105, p. 54-63 (13 April 2006).

10 Article 51(2) titled "Scope of Guaranteed Rights" enshrines that "Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others."

recognised that

> "the persons whose data have been retained [must] have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access and use of that data."[11]

In its analysis the CJEU explained that the 2006 Directive included within its scope all persons, all means of communication and all traffic data without differentiations or limitations, that it did not provide for satisfactory limits to access by the competent national authorities, and that it did not tailor data retention periods to the goals or categories of crime concerned. The Directive therefore failed to meet human rights standards in the EU. As a result of the *Digital Rights Ireland* judgment, all national implementing legislation transposing Directive 2006/24 into national law is no longer compliant with EU law. Member States have had to repeal and amend their laws, but some Member States have not yet done so.

In December 2016, the CJEU in *Tele-2/Watson* reaffirmed *Digital Rights Ireland* and expanded on it. The judgment positively asserted minimum safeguards of EU law that must be prescribed in any national data retention legislation. The CJEU held that the Charter of Fundamental Rights of the European Union must be interpreted as precluding:

> "national legislation which, for the purpose of fighting crime, provides for general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication, [and] national legislation governing the protection and security of traffic and location data and, in particular, access of the competent national authorities to the retained data, where the objective pursued by that access, in the context of fighting crime, is not restricted solely to fighting serious crime, where access is not subject to prior review by a court or an independent administrative authority, and where there is no requirement that the data concerned should be retained within the European Union."[12]

The Court further elaborated on the requirements to be fulfilled by national data retention legislation in order for it to be lawful:

> "Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, does not prevent a Member State from adopting legislation permitting, as a preventive measure, the targeted retention of traffic and location data, for the purpose of fighting serious crime, provided that the retention of data is limited, with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted, to what is strictly necessary.
>
> In order to satisfy the requirements set out in the preceding paragraph of the present judgment, that national legislation must, first, lay down clear and

[11] Digital Rights Ireland Case, supra note 1, at para. 54.
[12] Tele-2/Watson Case, supra note 2, at para. 134.

precise rules governing the scope and application of such a data retention measure and imposing minimum safeguards, so that the persons whose data has been retained have sufficient guarantees of the effective protection of their personal data against the risk of misuse. That legislation must, in particular, indicate in what circumstances and under which conditions a data retention measure may, as a preventive measure, be adopted, thereby ensuring that such a measure is limited to what is strictly necessary (see, by analogy, in relation to Directive 2006/24, the Digital Rights judgment, paragraph 54 and the case-law cited).

Second, as regards the substantive conditions which must be satisfied by national legislation that authorises, in the context of fighting crime, the retention, as a preventive measure, of traffic and location data, if it is to be ensured that data retention is limited to what is strictly necessary, it must be observed that, while those conditions may vary according to the nature of the measures taken for the purposes of prevention, investigation, detection and prosecution of serious crime, the retention of data must continue nonetheless to meet objective criteria, that establish a connection between the data to be retained and the objective pursued.

In particular, such conditions must be shown to be such as actually to circumscribe, in practice, the extent of that measure and, thus, the public affected.be based on objective evidence which makes it possible to identify a public whose data is likely to reveal a link, at least an indirect one, with serious criminal offences, and to contribute in one way or another to fighting serious crime or to preventing a serious risk to public security. Such limits may be set by using a geographical criterion where the competent national authorities consider, on the basis of objective evidence, that there exists, in one or more geographical areas, a high risk of preparation for or commission of such offences."[13]

Moreover, the Court specified that providers of electronic communications services must put measures in place to ensure the security and integrity of the retained data. In particular they must:

"take appropriate technical and organisational measures to ensure the effective protection of retained data against risks of misuse and against any unlawful access to that data. Given the quantity of retained data, the sensitivity of that data and the risk of unlawful access to it, the providers of electronic communications services must, in order to ensure the full integrity and confidentiality of that data, guarantee a particularly high level of protection and security by means of appropriate technical and organisational measures. In particular, the national legislation must make provision for the data to be retained within the European Union and for the irreversible destruction of the data at the end of the data retention period."[14]

[13] Id., at paras. 108-111.
[14] Id., at para. 122.

Data Retention under European and International Human Rights Law

All EU Member States are also parties to the European Convention on Human Rights and Fundamental Freedoms and to the International Covenant on Civil and Political Rights (ICCPR), both enshrining the right to privacy. In its jurisprudence, the European Court of Human Rights has reflected on some key aspects of data retention.[15] In its ruling in Roman Zakharov v. Russia, the Court emphasised the need for safeguards, in particular clear and proportionate rules about storage and destruction of data:

> "The Court considers the six-month storage time-limit set out in Russian law for such data reasonable. At the same time, it deplores the lack of a requirement to destroy immediately any data that are not relevant to the purpose for which they has been obtained. The automatic storage for six months of clearly irrelevant data cannot be considered justified under Article 8.
>
> Furthermore, as regards the cases where the person has been charged with a criminal offence, the Court notes with concern that Russian law allows unlimited discretion to the trial judge to store or to destroy the data used in evidence after the end of the trial. Russian law does not give citizens any indication as to the circumstances in which the intercept material may be stored after the end of the trial. The Court therefore considers that the domestic law is not sufficiently clear on this point..."[16]

The Human Rights Committee, in interpreting Article 17 of the ICCPR, has similarly adopted a position that data retention policies constitute an interference with the right to privacy and that as a general rule countries should "refrain from imposing mandatory retention of data by third parties".[17] In its concluding observations, including to some EU Member States, the Human Rights Committee has elaborated on the safeguards required to ensure compliance with the ICCPR. The Committee has particularly noted that Member States should review their data retention regimes with the view of ensuring:

> "that such activities conform with its obligations under article 17 including with the principles of legality, proportionality and necessity; [and that there exist] robust independent oversight systems [...] including by providing for judicial involvement in the authorization of such measures in all cases and affording persons affected with effective remedies in cases of abuse, including, where possible, an ex post notification that they were subject to [these] measures."[18]

15 Rotaru v. Romania, App. No. 28341/95, European Court of Human Rights, Judgment, para. 46 (4 May 2000); Weber and Saravia v. Germany, App. No. 54934/00, European Court of Human Rights, Decision on Admissibility, para. 132 (29 June 2006); Kennedy v. The United Kingdom, App. No. 26839/05, European Court of Human Rights, Judgment, paras. 64-65, 162-163 (18 May 2010).

16 Roman Zakharov v. Russia, App. No. 47143/06, European Court of Human Rights, Judgment, paras. 255-256 (4 December 2015).

17 Concluding Observations of the Fourth Periodic Report of the United States of America, Human Rights Committee, U.N. Doc. CCPR/C/USA/CO/4, para. 22 (23 April 2014).

18 Concluding Observations on the Sixth Periodic Report of Italy, UN Human Rights Committee, U.N. Doc. CCPR/C/ITA/CO/6, para. 37 (28 March 2017). See also Concluding Observations on the Seventh Periodic Report of the United Kingdom of Great Britain and Northern Ireland, Human Rights Committee, U.N. Doc. CCPR/C/GBR/CO/7, para. 24 (17 August 2015); Concluding Observations on the Initial Report of South Africa, Human Rights Committee, U.N. Doc. CCPR/C/ZAF/CO/1, paras. 42-43 (27 April 2016).

These views are also reflected in the positions of UN independent human rights experts. In June 2014, the United Nations High Commissioner for Human Rights, expressed the view that:

> "Concerns about whether access to and use of data are tailored to specific legitimate aims also raise questions about the increasing reliance of Governments on private sector actors to retain data "just in case" it is needed for government purposes. Mandatory third-party data retention – a recurring feature of surveillance regimes in many States, where Governments require telephone companies and Internet service providers to store metadata about their customers' communications and location for subsequent law enforcement and intelligence agency access – appears neither necessary nor proportionate."[19]

In May 2015, the U.N. Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye, noted that:

> "Broad mandatory data retention policies limit an individual's ability to remain anonymous. A State's ability to require Internet service and telecommunications providers to collect and store records documenting the online activities of all users has inevitably resulted in the State having everyone's digital footprint. A State's ability to collect and retain personal records expands its capacity to conduct surveillance and increases the potential for theft and disclosure of individual information."[20]

Since the *Tele-2/Watson* judgment, EU member states had some discussion about how to review their data retention laws in light of this judgment.[21] The results of a questionnaire to EU member states on this issue give some indication of governments' position to date.[22] It is worth noting that the EU legal service which was mandated to provide an opinion on the matter noted that:

> "This judgment will have consequences on national data retention schemes in other Member States, which are considered to be an important tool in the fight against serious crime including terrorism. Existing national laws will need to be checked against this judgment, although this is likely to be difficult.

It is however clear from the operative part of the Tele2 judgment that a general and indiscriminate retention obligation for crime prevention and other security reasons would no more be possible at national level than it is at EU level, since it would violate

19 Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, U.N. Doc. A/HRC/27/37, para. 26 (30 June 2014).

20 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, U.N. Doc. A/HRC/29/32, para. 55 (22 May 2015). See also Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue, U.N. Doc. A/HRC/23/40, para. 95 (17 April 2013) ("States should ensure that communications data collected by corporate actors in the provision of communications services meets the highest standards of data protection").

21 Council of the European Union, Outcome of Proceedings, 6159/17 (3 Feburary 2017), available at http://data.consilium.europa.eu/doc/document/ST-6159-2017-INIT/en/pdf.

22 Council of Europe, General Secretariat of the Council, Note on Retention of Electronic Communications Data, 6726/1/17 Rev.1 (7 March 2017), available at http://www.statewatch.org/news/2017/mar/eu-council-datret-6726-REV-1-17.pdf.

just as much the fundamental requirements as demonstrated by the Court's insistence in two judgements delivered in Grand Chamber."[23]

The European Commission also indicated that it "intends to elaborate guidance as to how national data retention laws can be constructed in conformity with the judgement."[24]

Member State Laws post *Tele-2/Watson*: the current State of Affairs

The *Digital Rights Ireland* judgment has led, in some EU Member States, to the repeal and amendment of the national data retention legislation that transposed Directive 2006/24 into national law.[25] In a few of these jurisdictions, such as the Netherlands and Slovakia for example, the repeal of the pre-*Digital Rights Ireland* regime by national courts has led to a gap in the law as there is currently no designated data retention regime in place in those jurisdictions. **What has emerged from our analysis is that as a rule of thumb repeal or amendments to data retention legislation have mainly occurred as a result of challenges in national courts, predominately by human rights NGOs, while Governments and legislators have been largely inactive.** An exception to this is Luxembourg where the response to *Digital Rights Ireland* has come directly from the Ministry of Justice which formulated a new bill in 2015, however the bill is not yet in force.

The most concerning fact, however, is that in an alarmingly large number of Member States (roughly 40% of all countries surveyed in this report) the pre-*Digital Rights Ireland* regime transposing Directive 2006/24 is still in place.[26] In such countries the data retention regime has not yet been invalidated nor has new legislation been passed. In Portugal, Hungary, Spain and Cyprus, for instance, courts have been interpreting *Digital Rights Ireland* compatibly with their national legislation. In Ireland, the pre-*Digital Rights* regime is still the subject of litigation in the national courts and no new legislation has come into force. In countries such as Poland or the Czech Republic,[17] courts have recognised the national regimes' flaws but have not invalidated them. In Poland, amendments were subsequently made to the law but they appear even more restrictive to privacy than under the prior regime. In the Czech Republic, the old regime is still in place in spite of the Constitutional Court's reservation. **Countries that have failed to invalidated their old data retention regimes and are still reflecting the 2006/24 Directive, are clearly in breach of their obligations under EU law. The situation in these countries is analogous to the pre-*Tele-2/Watson* situation in Sweden and the UK, a situation which the CJEU held was unlawful despite governmental attempts to justify the legal regimes.**

23 Council of Europe, Information Note concerning the Tele2 and Watson Judgment, 5884/17 (1 February 2017) https://cdn.netzpolitik.org/wp-upload/2017/05/rat_eu_legal_service_vds_20170201.pdf.

24 COE Outcome of Proceedings, supra note 20, at p. 6.

25 See e.g. the United Kingdom, the Netherlands, Germany, Austria, Belgium, Luxembourg, Slovenia and Slovakia.

26 See e.g. Croatia, Cyprus, Czech Republic, France, Ireland, Poland, Portugal, Spain.

27 About 10% of all jurisdictions considered.

Even in Member States where the prior regime has been invalidated in the national courts and where new data retention legislation has come into force after *Digital Rights Ireland*, national laws are nonetheless inconsistent with the CJEU's most recent ruling in *Tele-2/Watson* (about 20% of all countries surveyed in this report).[28] In those countries the regimes might allow indiscriminate retetntion of data in bulk or provide vague and ill-defined regulation on access to that data by relevant authorities. Similarly, in the UK and Sweden litigation is still underway and no amendments to the current regime have yet been made. Data retention legislation is being considered or is on hold in about 30% of the jurisdictions surveyed, and in about half of these cases attempts to ensure compliance with *Tele-2/Watson* are being pushed.[29] Nonetheless, we are now 8-months into the CJEU decision, and the slow pace by which changes are evolving in these jurisdictions is concerning, given how impactful these data retention regimes are on Europeans' fundamental rights and freedoms.

It is evident that in most of the countries Privacy International has surveyed, change is being promoted through litigation by human rights NGOs instead of through proactive reform of the laws by Parliament. Legal proceedings are currently under way in about 35% of all countries considered, including Cyprus, Belgium, Sweden, Ireland, Germany, the U.K. and France. Nonetheless, in the course of these proceedings we have seen some alarming attempts by Governments to water-down the CJEU's judgments through improper interpretation. In other countries, such as Spain, we have witnessed open-defiance to the CJEU by making statements that pre-*Digital Rights Ireland* domestic laws are still in compliance with EU principles.

[28] See e.g. Bulgaria, Belgium, Romania, and Italy.

[29] See e.g. Austria, Belgium, Luxembourg, The Netherlands, Slovenia, Slovakia.

Conclusions and Recommendations

In *Tele-2/Watson* the CJEU not only confirmed the importance of its ruling in *Digital Rights Ireland* but expanded on that ruling, affirming positive requirements that national data retention legislation must fulfil in order to comply with both European and international human rights law. Member States have an obligation to ensure that their laws comply with the CJEU's jurisprudence, and EU law more generally. It is thus concerning to notice that only a limited proportion of Member States have actually annulled their pre-*Digital Rights* legislation and that practically no Member States' laws currently comply with Tele-2/Watson. Very few governments have taken the lead in pushing legal reforms, and to the extent that limited positive changes at the national level have occurred, they have been the result of litigation initiated by NGOs and other small interest groups.

Privacy International welcomes further court and legislative action in all EU Member States and encourages all governments to review and amend their data retention regimes in light of the CJEU's recent case-law. Member States must ensure that their data retention regimes are compliant with the principles of legality, necessity and proportionality, and provide sufficient safeguards from abuse, as emphasised in both *Digital Rights Ireland* and the *Tele-2/Watson* judgments. Privacy International also welcomes more dialogue amongst stakeholders and encourages the exchange of information on the legal situation in all EU jurisdictions.

National Data Retention Policies pre- and post *Tele- 2/Watson* (7 July 2017)

Country	Retention Policies Pre-Watson	Retention Policies Post-Watson
Austria	In 2009, the European Commission began proceedings against Austria for breaching EU law by failing to implement the DR Directive. These proceedings resulted in the CJEU ruling against Austria in 2010.[1] Following insufficient action by Austria, the Viviane Reding (Vice-President of the European Commission, EU Justice Commissioner) demanded that Austria finally implement the DR Directive or face stiff charges.[2] On 17 October 2011, AKVorrat.at (now known as epicenter.works) and two other parties launched a citizens initiative petitioning for the stopping of data retention and the abolition of the DR Directive.[3] By April 2012, the initiative had received 106,067 signatures.[4] Notwithstanding civil society criticisms, Austria implemented the DR Directive on 01 April 2012.[5] In response, AKVorrat.at along with Albert Steinhauser (National Councilor, Green Party Speaker) launched a constitutional complaint against data retention. Online, one could also register as a co-founder at draftsklage.at. In the end, 11139 individual complaints were filed. This joint action was subsequently submitted in the Austrian Constitutional Court on 15 June 2012.[6] In mid-December 2012, the President of the Court voiced doubts about the DR Directive's compatibility with the European Charter of Fundamental Rights.[7] Following the invalidation of the Directive in the EU Digital Rights Ireland Case and a public hearing at the Austrian Constitutional Court on 12 June 2014, the Austrian Constitutional	In January 2017, the Austrian Government agreed on new surveillance plans to monitor data and launch the "Arbeitsprogramm" ('Quick Freeze') security programme which would require telecoms to retain data for up to 12 months; the Prosecutor's office can then access this data for investigations. If the Prosecutor's suspicions are not confirmed, the suspect is to be informed. As summarised by newspaper der Standard, [translated from German]: "The monitoring method is based on the fact that telecom companies store some data for billing purposes anyway. The freezing process is intended to prevent this information from being routinely erased. However, the storage periods of the individual companies are inconsistent."[9] In early February 2017, the Green Party in Austria expressed strong criticism of Interior Minister Wolfgang Sobotka for his "roughly unconstitutional plans".[10] The current coalition Government split up in May 2017 and there will subsequently be elections in October 2017. Which measures of the security package will be implemented is presently unclear. Regardless, there is a possibility of two legislative amendments to: • the Security Police Act (Sicherheitspolizeigesetz), including access to private CCTV data without reasonable suspicion of a crime (for "prevention") and scanning and processing of registration numbers and • the Criminal procedure code, including elements of the the Quick

See end notes on page 43.

Country	Retention Policies Pre-Watson	Retention Policies Post-Watson
Austria (cont'd)	Court declared the DR Directive to be unconstitutional and annulled data retention law in Austria.[8]	Freeze model (will provide access to communications data, under judicial overview; can be retained up to twelve months from the moment the public prosecutor calls for it for a distinct suspect). Further, there are chances, that Government malware to monitor e2e-encrypted internet based communication will be introduced and regulated.[11] Epicenter.works is taking legal action concerning the "State Protection Act" (Polizeiliches Staatsschutzgesetz). This act allows law enforcement authorities to access communications data for crime prevention. Under the Austrian Constitution, judicial overview is required to access content data, but not to access metadata of communications – under the Act, not a judge, but a "legal protection officer" grants access to metadata.
Belgium	On 11 June 2015, the Belgian Constitutional Court annulled the data retention regime under the "loi du 30 juillet 2013" which provided for retention of data in accordance with Directive 2006/24, in turn invalidated by the CJEU in Digital Rights Ireland. It did so in response to two actions: respectively an action for partial annulment of the law by the Order of French and German speaking Belgian Lawyers, and an action for full annulment brought by the ASBL «Liga voor Mensenrechten» and ASBL «Ligue des Droits de l'Homme».[12] The annulled Belgian regime,[13] which was held to be too indiscriminate to comply with EU law, required Belgian service providers to retain customer metadata such as call logs, location and also internet data for a duration of one year for law enforcement to use when investigating serious crimes and terrorism. As a result of the Constitutional Court's judgment, the Belgian data retention legal framework has been recently amended by the "loi du 29 mai 2016 relative	Following the decision of the European Court of Justice in Tele 2/Watson, four claims have been introduced before the Constitutional Court for the annulment of the new Belgian regime on data retention. A decision from the Constitutional Court is expected towards the end of 2017. In parallel, the Belgian Government is currently investigating possible implications of Tele2/Watson.[17]

See end notes on page 43.

Country	Retention Policies Pre-Watson	Retention Policies Post-Watson
Belgium (cont'd)	aux communications électroniques" published on 18 July 2016.[14] The new law makes the following changes to prior Belgian data retention policy:[15] differentiation on the ground of three categories of data: subscriber data, connection and localization data, and traffic data, the latter two categories being less easily accessible than the first category; retention remains of one year but reinforcement of the safeguards and conditions for access to the data, which includes a differentiation of data accessible on the basis of the seriousness of the crime: for less serious crimes (ie. crimes with maximum penalties of less than a year of imprisonment or no imprisonment) only identification data will be accessible and only for the six-month period preceding the demand; for more serious crimes all three categories of data will be accessible, but connection and localization data and traffic data only accessible respectively for a period of six-months for penalties of 1 to 5 years of imprisonment, a period of nine months for more serious offences falling short of terrorism and for a year for terrorism-related offences; reinforcement of the measures to be taken by service providers to secure the data and the access to those data, and also the creation of a database for storage of retained data.[16]	
Bulgaria	On 19 March 2008, Access to Information Programme (AIP) filed an appeal in the Bulgarian Supreme Administrative Court against Article 5 of the Bulgarian Regulation #40 which implemented the DR Directive and allowed "passive access through a computer terminal" to retained data, as well as providing	Bulgaria's Prime Minister resigned in late 2016 and elections were held this year. The centre-right GERB party were reported in late March to have won.[21] There appears to have been no significant response to Tele 2/Watson.

See end notes on page 43.

Country	Retention Policies Pre-Watson	Retention Policies Post-Watson
Bulgaria (cont'd)	access without judicial permission to "security services and other law enforcement bodies". The Court held that Article 5 did not specify limits to data retention, including with regards to data retention by investigative bodies such as the the Prosecutor's office, and did not guarantee the protection of the right to privacy as per Article 32 of the Bulgarian Constitution.[18] Following the Digital Rights Ireland Case, Bulgarian's national ombudsman Konstantin Penchev, filed a challenge against data retention law in Bulgaria's Constitutional Court. Subsequently 12 March 2015, the Court annulled the law, declaring "law requiring telecommunications service providers to retain user data for at least a year to aid national security and other criminal investigations" to be void.[19] Subsequently, Bulgarian MPs passed amendments to the Electronic Communications Act at second reading on March 26 to replace the data retention provisions scrapped by the Court. Under the amended law, telecoms will have to collect traffic data and store it for a period of 6 months. Such data could only be used "in the interests of national security" or to investigate and prevent serious crimes, with the law also expressly prohibiting the retention of any data about the contents of electronic communication. Law enforcement agencies would require a court order to access the carrier data, with every such request logged in a register that would not be made public. The destruction of collected data would be overseen by Bulgaria's personal data protection watchdog and the courts.[20]	
Croatia	An October 2015 report by EuroJust confirmed that Croatia's data retention regime is still in place despite the 2014 CJEU ruling.[22] There is little information to suggest that its status has since changed.	Following an election in 2015, Croatia held another election in September 2016. Reports on 27 April 2017 suggest that the current coalition may call another election (though this is unlikely).[24]

See end notes on page 43.

Country	Retention Policies Pre-Watson	Retention Policies Post-Watson
Croatia (cont'd)	EDRi collaborated with other NGOs to analyse whether the data retention regimes of select member states complied with the 2014 CJEU ruling. It identified Croatia's key legislation as: Act on Electronic Communications; Regulation of the Government of the Republic of Croatia on obligations in the field of national security of the Republic of Croatia for legal and natural persons in telecommunications; and, Act on security and intelligence system in the Republic of Croatia. The analysis concluded that: the national provisions are indiscriminate; have a retention period of 12 months regardless of the types of data; exempt the irreversible destruction of certain data if processed and retained by "competent bodies" (presumably security related); and, does not expressly "require that the data must be retained within the EU".[23] Owing to limited accessible information available beyond this, a possible indicator of the Croatian Government's more current attitude towards privacy matters may be derived from Croatia being one of only four member states that abstained from the 2016 vote to replace the Safe Harbor framework with the Privacy Shield.	There appears to have been no significant response to Tele 2/Watson.
Cyprus	Cyprus adopted Law 183 (I) / 2007 (Retention of Telecommunication Data for Purposes of Investigation of Serious Criminal Offences Law of 2007) on 31 December 2007 to implement the DR Directive. The Supreme Court of Cyprus held on 01 February 2011 that Articles 4 and 5 of the 2007 data retention law were unconstitutional and that overall, the law appeared to go beyond the scope of the DR Directive.[25] It ruled that retained data can only be accessed "in cases of convicted and unconvicted prisoners and business correspondence and communication of bankrupts during the bankruptcy	No legislative changes have been brought since Tele 2/Watson. Mr Michalis Pikis filed an appeal against the Paphos SMS case. Pending the appeal, the Tele 2/Watson decision was issued. Before the hearing of the appeal, in view of the Tele 2/Watson decision, the Attorney General discontinued the prosecution of the accused in the Paphos SMS case. As a result, the appeal was also withdrawn since it became devoid of substance i.e., the criminal case in relation to which the disclosure orders were made was discontinued and the accused were discharged and acquitted of all charges.

See end notes on page 43.

Country	Retention Policies Pre-Watson	Retention Policies Post-Watson
Cyprus (cont'd)	administration", as per Article 17 of the Constitution.[26] Following the Digital Rights Ireland Case, in 2014, defence lawyers including Mr Michalis Pikis in the 'Paphos SMS trial' filed in the Supreme Court (first instance) an application for a writ of Certiorari in order to annul the District Court orders for disclosure of telecommunication data of their clients. The annulment of the disclosure orders would have prevented the prosecution from using essential evidence had been collected through retained data, as well as raising other privacy related concerns. On appeal after national courts found the use of retained data to be proportionate, the Cypriot Supreme Court ruled that the Constitution, as amended, permits authorities to access personal data "when this is necessary for the security of the Republic, as well as for averting, investigating or prosecuting serious criminal offences".[27] Further, it held that even if EU law was applicable, the existence of a judicial control mechanism for access to the retained telecommunication data satisfied the decision of the ECJ in the Digital Rights Ireland Case. Data of suspects, in the context of 'security' and 'investigations and prosecutions', and in cases of very serious offences punishable by a minimum term of 5 years' imprisonment, can be retained for 6 months. Access to retained data must be approved by a Prosecutor.[28] Commenting on data retention in Cyprus, the EU summarised in 2016: "…Law for access to recorded data which contain private communications was approved by the House of Representatives and is in force now. The following investigative techniques are permissible under national law:	More recently in Re Artemis Kolos (Application 1/2017) decision dated 31.01.2017, the Supreme Court rejected an application for a writ of Certiorari to annul an order granted by the District Court for the disclosure by a service provider of the IP address of the applicant, on suspicion of possession and distribution of child pornographic material. The Court held that the disclosure order in question (a) did not violate Article 15(1) of Directive 2002/58/EU or the Charter of Fundamental Rights of the Fundamental Rights, (b) the case law as it evolved with the decision in Tele 2/Watson, did not aim to cover this kind of interference (into the rights of suspects); the question as raised in Tele 2/Watson did not concern the application of Directive 2002/58/EU to persons such as the applicant; the questions raised therein concerned the policy that should govern service providers, (c) access to personal data is not contrary to the principle of proportionality provided it is approved by the relevant (judicial) authority as was propounded in Tele 2/Watson and it targets the prevention of serious crime. In the above decision, the Court commented that the CJEU in Tele 2/ Watson did not explain how there could be preventive control so that service providers retain only the data of those involved in serious criminal activities. The Court asked how in cases of child pornography there can be targeted preventive control of the data of a citizen of a member state without a criminal past or record, who downloads and distributes pornographic material, since detection of the pornographic material by international organisations is made only after a person gains possession of it. An appeal filed against this decision is pending. One of the basic grounds of appeal is that the first instance

See end notes on page 43.

Country	Retention Policies Pre-Watson	Retention Policies Post-Watson
Cyprus (cont'd)	• search and seizure of information systems/computer data; (Code of Criminal Procedure) • preservation of computer data; (Law 22(III)/2004) • order for stored traffic/content data; however, only for stored traffic data (Law 183(I)/2007) • order for user information. (Law 183(I)/2007). National law does not allow for real-time interception/ collection of traffic/content data. However, Law 183(I)/2007 forces ISPs to store telecommunication and traffic data for the purpose of investigation for a period of six months."[29]	judge misinterpreted and/or wrongly applied the Tele 2/Watson decision and that the disclosure orders in question violate the Charter of Fundamental Rights.[30]
Czech Republic	On 31 March 2011, having received a complaint from NGO Iuridicum Remedium (IuRe), the Czech Constitutional Court declared bulk data retention law, found in Sections 2 and 3 of the 2005 data retention provisions of Electronic Communication Act, to be unconstitutional. According to the Court, it would be necessary to consider each individual case where data had been requested.[31] Another decision by the Constitutional Court in December 2011 found the procedure of obtaining and retaining data "to be too vague, in breach of proportionality rule (its second step) and thus unconstitutional due to interference with right to privacy and informational self-determination".[32] Subsequently, the Czech Government drafted amendments to the 2005 Electronic Communication Act and related laws, which though was "better than the repealed regulation", it still contained "a number of errors that will lead to unconstitutional interference with the privacy of citizens",[33] including reinstating certain amended data retention provisions to reflected the DR Directive. Following the Digital	Currently, the Czech Republic is drafting amendments to the Act reconciling military intelligence and other laws which may affect data retention.[39] Further, there is no political will to respond to Tele 2/Watson. Quite the opposite, the Government has expressed inability to comply with the Court's ruling for targeted retention.[40] Further, a Parliamentary election will be taking place in October 2017.[41]

See end notes on page 43.

Country	Retention Policies Pre-Watson	Retention Policies Post-Watson
Czech Republic (cont'd)	Rights Ireland Case, no significant changes were made in the data retention regime. "A legal or a natural person providing a public communications network or a publicly available electronic communications service is required to store the call detail record of telephony and internet traffic and transaction data for a period of 6 months by providing that the content of communication is neither stored nor transmitted."[34] Data retention can be accessed in individual cases[35] by the Police, Prosecuting Attorney's Office, Security Information Service (BIS), Military Intelligence Service and Czech National Bank.[36] Data subjects, whose data have been requested under the Criminal Code, must be informed. Where such data is requested by the intelligence service or the Czech National Bank, court permission must be sought.[37] IuRe commented that the new laws ignored the "current situation where the Police Act authorizes the police to use the data outside of criminal proceedings. Under the current Police Act, police officers may require data more or less without any limits, without court supervision and without any clearly defined and controlled processes".[38]	
France	The current French data retention scheme was put in place before the Digital Rights Ireland judgment.[42] It requires ISPs to delay by one year the deletion of the following information about their customers: a) identification information about communications senders and receivers; b) information about the communications terminals used; c) the technical characteristics including the date, time and duration of each communication; d) data relating to ancillary	The scheme in place before Digital Rights Ireland is still in force in France and is subject to a pending challenge to the entire French data retention scheme under décret n°2011-219 du 25 février 2011 and article R. 10-13 du code des postes et communications électroniques in the French Conseil d'Etat court. It was brought by Exegètes Amateurs in May 2015. CDT and Privacy International joined the case in February 2016. We are expecting the case to move forward, as the Rapporteur has submitted his/her opinion to the court and a draft decision (not available to the parties). The opinion and draft will now be

See end notes on page 44.

Country	Retention Policies Pre-Watson	Retention Policies Post-Watson
France (cont'd)	services requested or used and their providers. There is an obligation for ISPs to retain data identifying their users to each of their connections. Under Article 20 loi n. 2013-1168 of 18 December 2013, the French Defence Ministry and Home Office are allowed to access such retained information for purposes as broad as "national security", "the prevention of terrorism", the "preservation of the essential elements of France's economic and scientific potential."[43] The current scheme is currently the subject of litigation before the French administrative court. In February 2015, the Exégètes Amateurs brought a legal challenge before the French administrative court (Conseil d'Etat) based on Décret n° 2014-1576 of 24 December 2014 on administrative access to connection data.[44] They claimed that the decree was ultra vires following Digital Rights Ireland.[45] In February 2016, the Conseil d'Etat rejected the application and refused to make a preliminary reference to the CJEU in spite of the Exegètes' specific request to do so. On 1st July 2016 the Exegètes appealed the rejection to the European Court of Human Rights, which dismissed their request. On 6 May 2015, the Exégètes made a second application based on Digital Rights, this time challenging the entire data retention scheme provided for under French law.[46] The Conseil d'Etat has not yet issued a decision in this case.	assigned to a Réviseur. A hearing is to be expected in the near future. At the legislative and governmental level, there are no signs of imminent reform. It also appears that the French Intelligence apparatus is putting pressure on the French Government to lobby at EU level for Tele2/Watson to be interpreted in a vague fashion.[47]
Germany	The 2008 German law on data retention which transposed Directive 2006/24 into German law was nullified by the Federal Constitutional Court in 2010 (this judgment was quoted several times in the Advocate General's opinion	Whilst changes to the 2015 data retention regime are not currently being envisaged at the governmental or legislative levels, several constitutional challenges have been raised against it before the Federal

See end notes on page 44.

Country	Retention Policies Pre-Watson	Retention Policies Post-Watson
Germany (cont'd)	in Digital Rights Ireland). After that judgment, the government could not agree on a new law transposing the Directive for several years, which eventually led to the European Commission threatening to initiate proceedings before the CJEU. This struggle to pass new legislation in Germany was cut short by the CJEU nullifying the 2006 Directive in Digital Rights Ireland. On 18 December 2015, a new law was passed reintroducing data retention in Germany. The law introducesd a new section 113b to the German Telecommunications Act (Telekommunikationsgesetz), are very similar to the 2008 law. The Act applies to all providers of publicly available telecommunications services (with the exception of short-term providers like hotels or restaurants). Furthermore the law states that:[48] 1. the retention period has been shortened (to four weeks for location data and ten weeks for all other types of data). No justification is needed for the retention (indiscriminate collection). 2. Providers of publicly available telecommunication services must store traffic data, such as telephone number, date, time and information on the service used (including specific details for landline, mobile and Internet telephony). Providers of publicly available Internet access services must store the Internet Protocol (IP) address, a unique identification of the access point and the attributed user ID, as well as date and time of the Internet usage. Location data includes the identifier of the network cell used for a particular communication. Providers must delete data stored pursuant to the retention requirements without undue delay, but no later than one week, after the retention period expired. 3. Providers must make such data	Constitutional Court, relying on the new CJEU judgment in Tele 2/Watson. One such challenge was brought by the Munich Network Provider Spacenet, who was supported by eco, the German Association of the Internet Industry. Spacenet was challenging its obligation to store Internet data under the 2015 regime. The service provider's application for an interim decision was declined in first instance by the Cologne Administrative Court but was then reviewed by the Higher Administrative Court of the German state of Northrhine-Westfalia.[49] In a preliminary decision the Higher Administrative Court has relieved Spacenet of its obligations to retain traffic data. The Court found that the German law failed to meet the requirements laid down in the Tele-2/Watson decision, namely that the law allowed for "general and indiscriminate" retention of communications data. It remains to be seen what the results of the decision are. While the German traffic data retention obligations are in principle still valid for all other service providers except for the original claimant, the ruling is a very clear statement that the competent courts would not approve if the German regulator Bundesnetzagentur tried to enforce the retention rules. And to the contrary, even if telecommunication service providers were inclined to retain traffic data without objection, it is doubtful whether they have legal basis for the retention. Germany's Federal Networks Agency, Bundesnetzagentur, announced on 28 June 2017 that it would temporarily desist from taking measures to enforce data retention (section 113b German Telecommunications Act). In the view of Bundesnetzagentur, the court decision has an importance which transcends the individual case, which is why the enforcement of data

See end notes on page 44.

Country	Retention Policies Pre-Watson	Retention Policies Post-Watson
Germany (cont'd)	available to the police and prosecution on request, to enable the authorities to prosecute serious crimes or to prevent concrete risks for the body, life or freedom of a person. 4. Communication content is excluded from the retention and residency requirements. That includes data relating to E-Mails. 5. all retained data must be stored locally within Germany (also known as data localization or data residency) 6. Finally, the retention must comply with a particularly high standard of IT security. The law was scheduled to enter into effect on 1 July 2017.	retention is suspended until a final decision is made in the principal matter.[50] The original Court proceedings will also continue now. While the ruling of the Higher Administrative Court of North Rhine-Westphalia, which was made as a result of summary proceedings, is not challengeable as such, there are also the main proceedings which are still pending at the lower Administrative Court of Cologne. And in addition, there are also numerous other proceedings against the traffic data retention obligations in Germany, both before the Cologne Administrative Court and before the Federal Constitutional Court. At this time, none of these courts has submitted a case to the ECJ, but this will probably change now.
Hungary	Article 159/A was inserted into the Electronic Communications Act by Article 13 of Act 174 of 2007, which was adopted with the objective of transposing into Hungarian law the European Data Retention Directive pre-Digital Rights Ireland. It is notable that the requirements of Article 159/A essentially duplicate those laid down in the DRD as respects (i) the categories of data to be retained, including the requirement to retain data about unsuccessful calls (Article 5 DRD) and (ii) the purposes for which it is to be retained (to enable access by law enforcement agencies and the national security service). The DRD was declared unlawful by the CJEU in DRI such that the provisions of Article 159/A necessarily also fall to be declared unlawful (as noted by the Commissioner, considered below). Article 159A of the Electronic Communications Act requires service providers to retain a wide range of data arising from the use of fixed line and mobile telephones, internet access, internet e-mail and	A 2015 case to the Supreme Court brought by the Hungarian Civil Liberties Union (with ORG and Privacy International intervening) against two major service providers, in an attempt to force the Hungarian Constitutional Court to repeal the Hungarian Electronic Communications Act – was rejected. As a result the Law remains in effect.[53] On 17 July 2016 new surveillance and encryption rules embedded in Hungary's E-Commerce Act entered into effect. Companies subject to the new rules are required to retain certain metadata (such as user IDs, times of registration and access, and IP addresses) for one year and disclose such data in response to targeted data / surveillance requests from Hungarian authorities. Companies failing to follow the new rules face a new regulatory enforcement procedure and fines of up to HUF 10 million (approximately US$35.000) per offence.[54] The Hungarian Government has recently expressed the view that

See end notes on page 44.

Country	Retention Policies Pre-Watson	Retention Policies Post-Watson
Hungary (cont'd)	internet telephony by subscribers. It is understood that this includes personal data about the subscriber or user; the supply address and type of equipment used by the subscriber (in the case of fixed line telephony or fixed location internet access); data capable of identifying the parties to any communication including the IMEI and IMSI of the calling party and the receiving party of any communication; the date, start and end time of the communication or use of internet, email or internet telephony; intermediate subscriber/user numbers to which calls are routed through a call forwarding or transfer service; cell site information capable of identifying the geographical location from which a mobile telephone call is made; the date, time and location of any use of pre-paid anonymous services. The retention is of vast swathes of metadata, including in relation to persons for whom there is no suspicion of criminal behaviour or that they pose a threat to national security. The Hungarian legal provisions concerned contain no safeguards which might enable persons whose data have been retained to effectively protect their personal data against the risk of abuse and against any unlawful access and use of that data. The blanket nature of the data retention obligation (which appears to apply to all electronic communications providers and to all subscribers and service users) is such that it cannot meet the criticisms of the CJEU in Digital Rights Ireland. The obligation under Article 159/A of the Electronic Communications Act does not lay down the clear and precise rules that the CJEU has said are needed to govern the scope and application of the measure in question and to impose minimum safeguards including in relation to targeted retention, exclusion of persons whose communications are subject to professional secrecy, or	"Article 11 of the proposal for a new e-privacy Regulation could be an adequate response to the [tele-2/Watson] judgement of the Court at EU level. The wording of Article 11 is general enough to leave room for Member States to find various solutions in their national legislation, while it reflects properly on the requirements set out in the judgement. However, even on this basis, the challenge remains for national legislations to develop an effective and operative legal model consistent with the guarantees required by the judgement at the same time. There is a need for launching a more detailed guidance to Member States at EU level".[55]

See end notes on page 44.

Country	Retention Policies Pre-Watson	Retention Policies Post-Watson
Hungary (cont'd)	temporal limitations on retention periods ("strictly necessary" – the law allows for extensive retention periods, 6 months for unsuccessful calls and 1 year for all other data).[51] Police and the National Tax and Customs Office require prosecutor's authorisation. Prosecutor and national security agencies may access such data without a court order.[52]	
Ireland	Pursuant to a complaint filed by Digital Rights Ireland (DRI), the EU Court invalidated the DR Directive in 2014. The Communications (Retention of Data) Act 2011 is still in place with the Government arguing that the primary law did not delegate EU law and so it was not bound by the CJEU ruling. As per this 2011 Act, data relating to telephone and mobile data must be retained for 2 years, and internet data must be retained for 1 year. Data may be requested by the police, revenue and army subject to permission. There is limited judicial oversight, with the regime only requiring "a single paragraph annual report".[56] In January 2016, Digital Rights Ireland instructed its lawyers to serve legal papers on the Irish government, challenging whether the office of the Irish Data Protection Commissioner is truly an independent data protection Authority under EU law.[57] In January 2016, a review of these laws was launched "after it emerged the Garda Síochána Ombudsman Commission (GSOC) had accessed records of two reporters following a complaint from a friend of the late Katy French. He had alleged information about the model's case had been leaked to the media by gardaí. There was concern about the ease with which the ombudsman and other agencies like An	DRI's legal challenge to invalidate the 2011 law, as well as preceding laws, has returned to Court and is currently subject to litigation.[59] The Irish Government has recently expressed critical views of the CJEU jurisprudence noting that: "When seen against Ireland's current model for regulating access to retained communications data for law enforcement services, the implications of the CJEU judgement in the Tele 2 case have the clear potential to seriously hamper the investigation of serious crime and protection against security threats".[60]

See end notes on page 44.

Country	Retention Policies Pre-Watson	Retention Policies Post-Watson
Ireland (cont'd)	Garda Síochána and the Defence Forces could access this kind of information under current legislation."[58] The review is ongoing and the Department of Justice is still to publish its report.	
Italy	The Italian Personal Data Protection Code establishes in Section 123(2) that providers "shall be allowed to process traffic data that are strictly necessary for contracting parties' billing and interconnection payments for a period not in excess of six months". Section 132 of the Act establishes an exception to that rule for purposes of crime prevention, noting that: "telephone traffic data shall be retained by the provider for twenty-four months as from the date of the communication with a view to detecting and suppressing criminal offences, whereas electronic communications traffic data, except for the contents of communications, shall be retained by the provider for twelve months as from the date of the communication with a view to the same purposes. The data related to unsuccessful calls that are processed on a provisional basis by the providers of publicly available electronic communications services or a public communications network shall be retained for thirty days."[61] In summary under Article 132 of the privacy law phone communications data may be retained for 24 months, internet metadata may be retained for 12 months and unanswered phone calls may be retained for 30 days.[62] In connection with investigations of serious crime, the Anti-Terrorism Decree,[63] as was amended on 24 February 2016 by a subsequent decree ("Milleproroghe" decree),[64] compels telecom operators to retain already collected data until 30 June 2017 and beyond the times allocated in the Personal Data Protection Code. Retention terms under Article 132 will then be either reinstated or prolonged	There has not been a renewal or extension of the clause in the Anti-Terrorism Decree. As a result all data collection retained for extended periods on the basis of that Anti-Terrorism Decree was supposed to be deleted after 30 June 2017, with retention corresponding with the original Section 132 of the Personal Data Protection Code. On 19 July 2017 the Lower House approved "Proposta emendativa 12-bis.020". Section 12-ter of the bill derogates from Section 132(1) by setting a retention period of 72 months (6 years) for both telephone and traffic data. The bill is now pending before the Senate before it can become a law.[66]

See end notes on page 44.

Country	Retention Policies Pre-Watson	Retention Policies Post-Watson
Italy (cont'd)	even further, as the Government has not yet indicated its intentions.[65] The Italian law imposes on Telecom providers obligations to engage in indiscriminate data retention, in stark contradiction with the jurisprudence of the CJEU. Moreover, the temporal limitations that were introduced in the Personal Data Protection Code have been cast aside through Governmental decrees, allowing for retention of data for even greater periods. That in itself constitutes a violation of the right to privacy. Even further, access to such data by the authorities is not subject to authorization from a judicial authority.	
Luxembourg	The Luxembourgish data retention regime in place before the CJEU's judgment in Digital Rights Ireland was contained in the Luxembourg Criminal Procedure Code (the Criminal Code) and in the Act of May 30, 2005 laying down specific provisions for the protection of persons with regard to the processing of personal data in the electronic communications sector (the 2005 Privacy Act).[67] It allowed ISPs to retain data on their users beyond a six-month data retention period. It also entitled judicial authorities to access the data retained by ISPs for the purposes of the investigation, detection and prosecution of any criminal offences subject to a criminal or correctional penalty of at least one year of imprisonment. In response to the CJEU's judgment in Digital Rights Ireland, on 7 January 2015 the Luxembourg Ministry of Justice filed with the Chamber of Deputies bill n° 6763 (the 2015 Bill) modifying the previous regime[68] and specifically concerning traffic data[69] and location data.[70] The Bill has not yet been passed and was intended to: Provide that judicial authorities could only access retained data for an exhaustive list of offences with a penalty of at least one year of	As of 25 July 2016, the 2015 Bill had not yet come into force.[73]

See end notes on page 44.

Country	Retention Policies Pre-Watson	Retention Policies Post-Watson
Luxembourg (cont'd)	imprisonment;[71] Compel service providers and operators to delete irrevocably and without delay the retained data after the 6 months required retention period; Increase the penalties for breach of those obligations; Provide that data must be stored within the territory of the European Union.[72]	
The Netherlands	The data retention legislation that existed prior to Digital Rights Ireland has been invalided by a Dutch court order in 2015.[74] Recently, the topic of data retention in the Netherlands was referred by Privacy First to the UN Human Rights Council as well as the UN Human Rights Committee in September 2016 and December 2016, respectively.[75]	At present no data retention regime is in place in the Netherlands. The Dutch government has made a proposal[76] attempting to re-introduce the obligation to retain data but the proposal has been put on hold because of Tele 2/Watson. The proposal has been currently put on hold and is waiting to be approved by the Dutch Senate.[77] The proposal is addressed to public telecommunication networks and service providers and relates to the retention of telecommunications data, including traffic data (including location data) and user-identification data in the Netherlands.[78] Fixed or mobile telephony including VOIP data must be retained for twelve months and internet access data for six months. As regards access: In cases of prosecution of serious crimes, information of the last six months may be obtained. In cases of prosecution of serious crimes with a minimum sentence of eight years, information retained for up to twelve months may be obtained. Such an order can be made by a prosecutor, after written prior approval of a magistrate. The information may also be obtained by both Dutch foreign and internal intelligence services and there is no time limit to information that can be accessed for that purpose.

See end notes on page 44.

Country	Retention Policies Pre-Watson	Retention Policies Post-Watson
The Netherlands (cont'd)		Service providers must ensure secure and centralized storage of the retained data in a room accessible only to authorized personnel and that the information is stored in the European Union.[79]
Poland	The DR Directive "was transposed into the Polish legal system in 2009 through the changes in the telecommunications Law, the Code of Criminal Procedure and a number of legal acts defining the powers of relevant law enforcement agencies", with data to be retained for 2 years. In 2011-2012, the Ministry of Administration and Digitalisation proposed a reduction of the retention period to 1 year and the change in access rules to the effect that only criminal courts would be able to use the retained data.[80] Following the Digital Rights Ireland Case, a group of senators proposed legislation for a new data retention regime. This project however was suspended until the 2014 verdict of the Constitutional Tribunal. On 30 July 2014 the Polish Constitutional Tribunal, at the request of the Ombudsman and Attorney General, ruled on Poland's data retention regime (and other surveillance powers). The tribunal did not consider whether data retention was unconstitutional as it was not included in the complaint, but did rule that access to retained data needs better independent oversight and well-defined safeguards. The Tribunal gave the Government 18 months to amend the law.[81] Subsequently on 7 February 2016, Poland passed a new data retention law that has been described as "very strict and intrusive surveillance law" ('Ustawa Inwigilacyjna'). Pursuant to this law, ISPs were required to share data collected by them in the same way as telecommunication operators, without real oversight.[82] "They will have to log and store the	It is concerning that in spite of the increased retention measures introduced in 2016, there has been no significant response to the CJEU's ruling in Tele 2/Watson.[84]

See end notes on page 45.

Country	Retention Policies Pre-Watson	Retention Policies Post-Watson
Poland (cont'd)	metadata about each internet user on their network for up to 2 years. The law also extends the scope of cases where access to the retained data is allowed, from aid to ongoing investigations to detection and prevention of crimes. As a result, one doesn't have to be an official suspect to be placed under surveillance for up to 18 months."[83]	
Portugal	The Portuguese law implementing the 2006 Directive, Law no. 32/2008, has not been repealed after the Digital Rights Ireland Case. In the 2015 Report No. 7 on traffic data retention and Law no. 32/2008, the Portuguese Public Prosecutor's Office explains that this was so because the Portuguese implementing instrument was deemed to comply with the criteria the CJEU laid out in Digital Rights Ireland.[85] Pursuant to the 2008 law, data may only be retained for serious crimes (including terrorism, organised crime, kidnapping, crimes against State security) and can be retained for up to 1 year. Data can be accessed by law enforcement subject to judicial permission. The New Cybercrime Law no. 109/2009 did not amend this.[86]	There has been no significant response to Tele 2/Watson. The Government of Portugal has recently expressed the following position: "Legislative amendments are not envisaged, since the legislation in force respects the case law of the Court of Justice, requiring that the retention and transmission of data can only take place for the exclusive purpose of investigating, detecting and prosecuting serious crimes and always requiring the intervention of the Investigating Judge, safeguarding the rights to data protection and to privacy enshrined in the Constitution of the Portuguese Republic".[87] Without prejudice to the above, there is one amendment which concerns access to stored date by Portuguese intelligence agencies (the Security Information Service (SIS) and the Information Service Strategic Defence Strategy (SIED)), as opposed to law enforcement. This is important to stress as the law grants external-facing agencies, which have no mandated role to play in the country's internal criminal process, access to metadata of Portuguese citizens. Decree No. 147/XII concerns access by these agencies to telecommunications data and internet data, covering 'basic data' (records necessary for the functioning of the network such as identifying details about the user's address and services), 'equipment location data' (records indicating the geographical position of the terminal equipment), 'traffic data' (data necessary for the

See end notes on page 45.

Country	Retention Policies Pre-Watson	Retention Policies Post-Watson
Portugal (cont'd)		purpose of sending a communication or for purposes of billing). Access to basic data and equipment location data is allowed for the purposes of protecting national defence, internal security, and the prevention of acts of sabotage, espionage terrorism, proliferation of weapons of mass destruction and highly organised crime. Access to traffic data is limited to the prevention of acts of espionage and terrorism only. Access includes "real time.. direct online access" to the required information. Each request for access requires judicial authorisation from a special committee that will form under Portugal's Supreme Court. The requests will be in writing and drawn up by the directors of SIS or SIED or their subordinates. The request must cover the concrete operational action to be carried out, the facts supporting the request, the identification of the person or persons targeted and the duration of the required measure (which may not exceed three months and could only be renewed once for a similar period). Any request to access will be communicated to the Prosecutor-General. The judicial review process will cover an examination of the necessity, adequacy and proportionality of the request, as well as whether less intrusive alternatives have been exhausted. The decisions will be granted within 48 hours from the moment the request is made. The law further envisions the creation of standards for access to be adopted by the Government ministers responsible for communication and information cybersecurity. The Informations Systems of the Portuguese Republic (SIRP), the parent body of the SIS and SIED will be provided access to this information on a "need to know" basis. The Supreme Court Committee will also have the power to cancel access or call for the destruction of certain data per its discretion. The Prosecutor General

See end notes on page 45.

Country	Retention Policies Pre-Watson	Retention Policies Post-Watson
Portugal (cont'd)		and the SIRP Data Supervisory Commission shall be notified of such decisions. Finally all data accessed by SIS and SIED shall be stored in their data centres and subjected to standards of protections including good faith access, chain of custody, confidentiality, and overall oversight by the SIRP Data Supervision Commission. The Commission will receive bi-monthly a list of applications for authorisation of access, may subject requests for clarification, and would also be in charge of any data subject requests by Portuguese citizens. The law has received final approval by the president, who will submit it to the Constitutional Court for a review of the bill's constitutionality.[88]
Romania	A first Romanian data retention law (298/2008) was declared unconstitutional by Romanian Constitutional Court decision 1258/2009. Subsequently, two judges from two different lower courts questioned ex officio whether a second Romanian data retention law 82/2012 which transposed Directive 2006/24/EC was unconstitutional. By decision no. 440 of 8 July 2014, the Court declared the second Romanian data retention law (no. 82/2012) unconstitutional. Article 5(1) of Law 235/2015, which modified Law 506/2004 (implementation of the eprivacy directive), states that there is no data retention obligation. Traffic data must be deleted or transformed in anonimised data when they are no longer necessary for communication transmission. Exceptions can be made however for the purposes of billing and interconnection (5(2)), marketing electronic communications services or for the provision of value added services (5(3)), whereby data may be retained for up to 3 years and data may be accessed by law enforcement and security bodies subject to applicable conditions.[89]	There has been no significant response to Tele 2/Watson.[92]

See end notes on page 45.

Country	Retention Policies Pre-Watson	Retention Policies Post-Watson
Romania (cont'd)	Two cases were raised in the Constitutional Court regarding the text adopted by the Law 235/2015, however the Court decided on both cases in decision 621 on 13.10.2016, that they were inadmissible. An article written by a Romanian Judge in February 2016 argued that the Law 235/2015 might not constitute the basis for Article 152 of the Criminal Procedure Code (which sets out applicable conditions for law enforcement and security bodies to access retained data). This would imply that access to already retained data might lack the formal legal basis.[90] Another article written by a Romanian lawyer analysed the Law 504/2006 (which includes an obligation for certain controllers to allow access of authorities to the traffic data they process) in light of Tele 2/Watson. The article concluded that the Romanian law was inconsistent with the decision because access to retained data is not limited to serious crimes, and authorities are not obligated to inform persons whose data has been accessed, even when this does not impede the investigation.[91]	
Slovakia	Prior to April 2015, the Slovakian data retention regime required providers of electronic communications to store indiscriminate traffic, localization data and data about the communicating parties, including unsuccessful calls, for a period of 6 months in the case of internet, email or VoIP communications or for a period of 12 months for other means of communication.[93] In April 2015, the Grand Chamber of the Constitutional Court (PL. ÚS 10/2014)[94] effectively invalidated Slovakia's existing data retention regime, giving effect to Digital Rights Ireland.[95] Following the CC's 2015 decision, the government prepared a draft act that	The new legislation does not seem to be in force yet. Under the current regime which consists of the parts of the old regime not invalidated by the Constitutional Court's ruling, traffic and location data must be destroyed or anonymized immediately after any communication has been finished.[97] An exception to this is the retention of data that is necessary for invoicing a customer, however even this data can be stored only for the extent and duration justified by the practice of invoicing.[98] Data retention, still regulated under the prior regime,[99] is now only allowed if approved by a court order. [100] [101]

See end notes on page 45.

Country	Retention Policies Pre-Watson	Retention Policies Post-Watson
Slovakia (cont'd)	aims to enhance control over the data retention process and clearly details the situations in which data can be retained, stored and requested by state bodies. Specifically, the proposed law permits this only for the most serious crimes, such as terrorism or threats to the integrity of the country.[96]	
Slovenia	Prior to July 2014, the Slovenian data retention regime required blanket data retention for a period of 8 months for internet related and 14 months for telephony related data. Government was entitled to access such data for purposes falling short of the investigation of serious crimes.[102] In March 2013, the Information Commissioner requested a constitutional law review of the regime. On 3 July 2014, the Constitutional Court of the Republic of Slovenia delivered its ruling abrogating the data retention provisions of the Act on Electronic Communications (ZEKom-1) in light of Tele 2/Watson, in particular as regards the above mentioned retention periods.[103] [104] In its judgment, the Court also requested that operators of electronic communications delete retained data immediately upon the judgment's publication in the Official Gazette. Thereafter, the residual required retention period for phone usage data became approximately 3-4 months of data for both major national providers, while internet usage data varied from operator to operator. The police kept existing technical arrangements in place, and was able to keep receiving phone traffic data through existing secure channels. The legal basis for requesting the data remained unaffected by the Constitutional Court's judgment.[105]	Currently, the situation is that the telecommunication operators normally store traffic data only for the period related to finalising any billing related activities (3-4 months). As stated during the meeting of the Working Party on General Matters and Evaluations of 3 February 2017 concerning the item on retention of electronic communication data,[107] a draft amendment to the Slovenian regime was proposed which should make the following changes to the Slovenian regime: • differentiated legal bases for each type of investigative measure used to obtain data on suspect electronic communications, • investigative judge can order existing telephone/internet data to be released by the service provider based on a state prosecutor's proposal supported by grounds, and can also order the telephone/internet provider to freeze a suspect's communications data for up to 3 months, provided the request is properly motivated, • court, police or state prosecutors can request telephone/internet providers to hand over data on their users/subscribers who are suspects in serious offences or information on the existence of their contract with the provider. • The proposed new bill should take into account the CJEU's Tele2/Watson judgment and also the CC's 2014 judgment.[108] It is currently in the process of being finalised and has

See end notes on page 45.

Country	Retention Policies Pre-Watson	Retention Policies Post-Watson
Slovenia (cont'd)	This regime is still currently in place. Subsequently, the Information Commission has issued guidelines on privacy impact assessments (PIA) for the introduction of new police measures.[106]	been tabled at the Parliament this spring. • Furthermore, Articles 149b – 154 of the Criminal Procedure Act[109] define the rules for access to the personal data stored by the telecommunication operators for the purposes of law enforcement. Those articles are also currently in the process of amendment; the amendment has already been tabled at the Parliament this spring.[110]
Spain	The current data protection regime is the Law 25 of 18 October 2007 (Ley de Conservación de Datos del Estado español 25/2007), updated by the Telecommunications General Law on 10 May 2014. In 2007, Asociación de Internautas brought a constitutional challenge to the law and the CC rejected it in 2008 (sentencia 44/2008 de 5 de febrero).[111] In 2014 criminal defence lawyers attempted to use the CJEU ruling Digital Rights Ireland to overturn convictions in cases where evidence has been collected via retained data. National courts held that data retention is a proportionate measure for combating crime. In relation to Digital Rights Ireland, the Court of Appeal explicitly stated that the invalidation of the Directive does not automatically make the national legislation unconstitutional.[112] Nonetheless, after the invalidation of the Data Retention Directive the Spanish data retention regime underwent some modifications including: an obligation that data transfers be made electronically and within seven calendar days of the relevant authority's request, sanctions imposed on the non-retention of data, divided into very serious, serious, and minor infractions.[113] [114]	The Spanish Data Retention law Act 25/2007 has not been modified to abide the ruling, and the requirements to Internet and telecommunications providers for general and indiscriminate retention and preservation of traffic and location data, from 6 months to 2 years, are still in force.[116]

See end notes on page 45.

Country	Retention Policies Pre-Watson	Retention Policies Post-Watson
Spain (cont'd)	The current regime applies to traffic and location data, as well as subscriber identification data, for legal entities and natural persons. It provides for a standard retention period of 12 months from the date of the communication, which could be extended to up to 2 years to reduced to 6 months by the government. Under Article 3 of the Law, the data to be retained is classified in the following categories: data necessary to trace and identify the source of a communication; data necessary to identify the destination of a communication; data necessary to identify the date, time and duration of a communication; data necessary to identify the type of communication; data necessary to identify users' communication equipment or what purports to be their equipment; and data necessary to identify the location of mobile communication equipment. Articles 6 and 7 provide that data should only be transferred by the operators to competent authorities if a judicial warrant in place. The law also included measure for keeping the data securely stored, as well as an obligation on mobile operators to keep a register of their prepaid card-holders' names.[115]	
Sweden	As stated by the Swedish Delegation during the meeting of the Working Party on General Matters and Evaluatons of 3 February 2017 concerning the item on retention of electronic communication data,[117] the existing Swedish Data Retention Act (LEK) was passed in 2003. It required telecommunications companies and ISPs to collect and retain metadata on the	We understand from recent Swedish input that:[121] • The Swedish Administrative Court of Appeal (Kammarrätten) will now need to apply the CJEU's preliminary ruling in the Watson/Tele 2 appeal at national level, • The CJEU ruling should have come

See end notes on page 45.

Country	Retention Policies Pre-Watson	Retention Policies Post-Watson
Sweden (cont'd)	calls and other communications of its customers, including metadata on the time, location, and duration of the communications, for a period of six months.[118] According to the CJEU in Tele 2/ Watson, "[o]n 29 April 2014, the justitieminister (Swedish Minister for Justice) appointed a special reporter to examine the Swedish legislation at issue in the light of the Digital Rights judgment. In a report dated 13 June 2014, entitled 'Datalagring, EU-rätten och svensk rätt, Ds 2014:23' (…), the special reporter concluded that the national legislation on the retention of data, as set out in Paragraphs 16a to 16f of the LEK, was not incompatible with either EU law or the European Convention for the Protection of Human Rights and Fundamental Freedoms".[119] Tele 2 Sverige, which had stopped collecting data on its customers, "considered that the 2014 report was based on a misinterpretation of the Digital Rights judgment and that the obligation to retain data was in breach of the fundamental rights guaranteed by the Charter, and therefore brought an action before the [Administrative Court in Stockholm]".[120] The CJEU's Tele2/Watson judgment effectively said that the existing Swedish data retention regime was incompatible with the EU Charter of Fundamental Rights.	as no surprise for Swedish lawmakers and authorities in light of Digital Rights, • The EC has announced they will coordinate again, • Alongside the Data Retention provisions based on the Directive, there is the e-privacy directive which as its main principle states that operators are to purge data if none of certain exceptions apply, such as for billing, etc; • The debate in Sweden, following the CJEU's ruling has been very un-nuanced. Some public officials have asked operators not to stop helping to fight crime', implying that operators who have stopped applying the provisions ruled invalid by the ECJ for being in breach of Human Rights, those operators are to blame for that crimes will now not be possible hinder and/or investigate; • Legislative initiatives to do with ePrivacy and narrower data retention obligations are being envisaged.
United Kingdom	The Data Retention and Investigatory Powers Act received Royal assent on 17 July 2014. DRIPA had been enacted in the wake of the Digital Rights Ireland decision as an emergency measure by the Government with very little scrutiny or debate in Parliament. It was passed as a matter of considerable alacrity to plug the hole created by the falling away of the data retention obligations derived from	The current data retention regime in the UK is a confusing mix following the Watson judgment; the implementation of transitional provisions in the Investigatory Powers Act; and an extension of the definition as to what it means to be a communications service provider and what can be retained under a communications data retention regime.

See end notes on page 45.

Country	Retention Policies Pre-Watson	Retention Policies Post-Watson
United Kingdom (cont'd)	the EU Directive as implemented by the UK. Section 1(1) of DRIPA provided that the Secretary of State may use a "retention notice" to require a public telecommunications operator to retain relevant communications data so long as the Secretary considers it necessary and proportionate for one of the purposes listed in the Regulation of Investigatory Powers Act of 2000 (e.g. national security, prevention of crime or disorder, in the interest of public safety or health, for the purposes of collecting taxes or other charges payable to a Government department, etc.) The retention of data envisaged by DRIPA is widespread, indiscriminate and not specifically targeted at a group of persons - according to the Government's witness evidence in the Watson litigation, targeted retention would defeat the purpose and utility of the regime. Furthermore Section 94 of the Telecommunications Act of 1984 further reaffirms the power of the Secretary of State to give directions of a "general character" to telecommunications operators as long as they are expedient in the interests of national security or relations with the Government of a country or territory outside the UK. The telecom operators must comply with such directions or they will be fined, and further are gagged from disclosing any information about the direction. This power has been utilized in respect of intelligence agencies gaining access to communications data.	Following the judgment, the case has been remitted back to the UK Court of Appeal. A hearing has not yet taken place. The government stated recently[122] that "…in light of the CJEU judgment, and in order to bring an end to the litigation, the Government have accepted to the Court of Appeal that the Act was inconsistent with EU law in two areas." However, until a hearing takes place, the details of what the Government is prepared to accept, the response to this from the Claimants' and ultimately what results from the CJEU's ruling is unknown. Furthermore, leaving the Divisional Court's Order in place as the 'last word' on the domestic lawfulness of the government's data retention regime, has a big impact. The Divisional Court's Order related solely to measures for accessing and using retained data. The Divisional Court made clear that they deemed a general indiscriminate data retention regime to be lawful if it was accompanied by a sufficiently limited access regime (paragraph 89 of the Divisional Court's judgment). This was not the ratio of the Watson/Tele2 judgment, in which the CJEU constrained the scope of both retention and access regimes. The House of Lords noted in their report {footnote same as above} that although DRIPA 2014 has expired, the CJEU's ruling potentially has ramifications for the Investigatory Powers Act ("IPA") 2016, which contains similar provisions to DRIPA. The partial implementation of the more expansive data retention powers in Part 4 of the IPA means that there is currently no independent oversight, no codes of practice and a statement from the Government that they will delay publication of the communications data Code of Practice

See end notes on page 46.

Country	Retention Policies Pre-Watson	Retention Policies Post-Watson
United Kingdom (cont'd)		to consider the Watson judgment. However, it was recently confirmed that Liberty has been granted permission to challenge Part 4 of the IPA which concerns data retention powers. What is clear, however, is that the Government continues to resist the full remit of the safeguards clearly laid out not only in Watson but also Digital Rights Ireland. That the Government is further resisting these safeguards in respect of the section 94 regime, whereby telecommunications operators are forced to provide a regular/ automatic feed of communications data to the intelligence agencies.

See end notes on page 46.

End Notes

1 http://www.internationallawoffice.com/Newsletters/IT-Internet/Austria/Schoenherr-Attorneys-at-Law/Austria-implements-EU-Data-Retention-Directive-at-long-last
2 http://derstandard.at/1297818369630/Druck-EU-Oesterreich-muss-Vorratsdatenspeicherung-umsetzen
3 https://www.parlament.gv.at/PAKT/PR/JAHR_2011/PK1243/
4 http://archiv.zeichnemit.at/
5 http://derstandard.at/1333184949199/Schauspiel-Vorratsdatenspeicherung-Ein-potemkinsches-Dorf
6 https://epicenter.works/sites/default/files/einbringung-akvorrat-vfgh-mai_2014.pdf; https://www.verfassungsklage.at/
7 https://epicenter.works/thema/vorratsdatenspeicherung
8 https://www.vfgh.gv.at/downloads/presseinformation_verkuendung_vorratsdaten.pdf
9 http://derstandard.at/2000051736311/Einfrieren-von-Vorratsdaten-und-WhatsApp-Ueberwachung-geplant
10 http://derstandard.at/2000052046259/Gruene-Mitterlehner-soll-obersten-Gefaehrder-Sobotka-austauschen
11 Wen received input from Epicenter.works.
12 See the judgment in French here: http://www.const-court.be/public/f/2015/2015-084f.pdf
13 Previous laws now modified: Loi du 13 juin 2005 relative aux communications électroniques – See Articles 126 and following + 145 (http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=2005061332&table_n ame=loi); Code d'instruction criminelle – articles 8 à 136quater – See Articles 46bis, 88bis and 90decies (http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=1808111730&table_n ame=loi) ; Loi du 30 novembre 1998 sur les services de renseignement et de sécurité – See Articles 13, 18/3, 18/8 (http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=1998113032&table_n ame=loi).
14 For more detailed clarifications on the content of the new Belgian data retention legislation, we can refer to the "exposé des motifs" that was published on the website of Parliament: http://www.dekamer.be/FLWB/PDF/54/1567/54K1567001.pdf
15 http://www.dekamer.be/FLWB/PDF/54/1567/54K1567001.pdf
16 See in particular Articles 126 and following at this link : http://www.ejustice.just.fgov.be/cgi_loi/loi_a1.pl?language=fr&la=F&cn=2005061332&table_name=loi&&caller=list&F&fromtab=loi&tri=dd+AS+RANK&rech=1&numero=1&sql=(text+contains+(%27%27))#LNK0066
17 See Belgian Delegation's submissions here: http://www.statewatch.org/news/2015/oct/eu-eurojust-analysis-ms-data-retention-13085-15.pdf
18 http://www.aip-bg.org/documents/data_retention_campaign_11122008eng.htm ; http://eulawanalysis.blogspot.co.uk/2014/04/national-legal-challenges-to-data.html
19 https://www.law360.com/articles/632375/bulgarian-court-latest-to-strike-down-data-retention-law
20 http://sofiaglobe.com/2015/03/26/bulgaria-scrambles-to-amend-scrapped-data-retention-provisions/
21 http://blogs.lse.ac.uk/europpblog/2017/03/27/2017-bulgarian-election-results-borisov-wins/
22 http://www.statewatch.org/news/2015/oct/eu-eurojust-analysis-ms-data-retention-13085-15.pdf
23 https://edri.org/files/DR_EDRi_letter_CJEU_Timmermans_20150702_annex.pdf
24 https://au.news.yahoo.com/world/a/35189654/croatia-pm-sacks-ministers-amid-fresh-election-talk/#page1
25 http://merlin.obs.coe.int/iris/2011/4/article14.en.html
26 http://www.cypruslawdigest.com/topics/technology-media-electronic/item/161-privacy,-data-retention-and-data-protection-in-the-electronic-communications-sector ; https://edri.org/edrigramnumber9-3data-retention-un-lawful-cyprus/
27 http://cyprus-mail.com/2015/10/27/telecoms-data-can-be-used-in-vergas-trial-supreme-court-rules/ ; http://fra.europa.eu/en/theme/information-society-privacy-and-data-protection/data-retention ; http://www.supremecourt.gov.cy/Judicial/SC.nsf/All/5B67A764B86AA78EC225782F004F6D28/$file/65-09.pdf (Greek)
28 https://www.efa.org.au/2015/07/29/european-data-retention-laws-update/ ; see also Re Matsias and another (2011) 1 CLR 152 and Re Andreas Isaias and another, Civil Appeal No 402/2012, decision 07.07.2014
29 http://data.consilium.europa.eu/doc/document/ST-9892-2016-REV-1-DCL-1/en/pdf
30 The information was compiled with input from Mr Michalis Pikis (Advocate).
31 https://edri.org/czech-decision-data-retention/
32 http://www.husovec.eu/2012/01/czech-constitutional-court-gives.html
33 https://edri.org/edrigramnumber10-15czech-republic-new-data-retention-law/
34 http://fra.europa.eu/sites/default/files/fra_uploads/czech-republic-study-data-surveillance-cz.pdf
35 https://www.bestvpnz.com/which-countries-have-the-worst-data-retention-laws/
36 http://www.lexology.com/library/detail.aspx?g=395a2e3a-d091-4723-a6db-0fac8c062660
37 http://www.statewatch.org/news/2013/dec/secile-data-retention-directive-in-europe-a-case-study.pdf

[38] https://edri.org/edrigramnumber10-15czech-republic-new-data-retention-law/ This runs in contradiction to Government's comments whereby they clarify that "It is important that police is limited in access to the data; there is no push method to some storage. Police can obtain data only under strict conditions and after approval of the court. We were of the opinion that this should protect the privacy as well as help police to investigate". http://www.statewatch.org/news/2017/mar/eu-council-datret-6726-REV-1-17.pdf.

[39] http://www.slidilove.cz content/k-navrhu-smirovaci-novely-zakona-o-vojenskem-zpravodajstvi-dalsich-zakonu

[40] http://www.statewatch.org/news/2017/mar/eu-council-datret-6726-REV-1-17.pdf ("We are analysing the judgement but we do not have any clear solution how to ensure targeted retention... from the technical point of view it is not easy to retain data just about persons convicted of a serious crime. It is even more difficult with the internet").

[41] This information was compiled thanks to Iuridicum Remedium.

[42] Décret n°2011-219 du 25 février 2011 and article R. 10-13 du code des postes et communications électroniques (CPCE) (https://exegetes.eu.org/recours/abrogationretention/demande/2015-04-27-demande.pdf) and Article 20 loi n. 2013-1168 du 18 décembre 2013 relative à la programmationmilitaire pour les années 2014 à 2019 (L.246-1 to L.246-5 code de la sécurité intérieure) (law on military planning) (https://www.legifrance.gouv.fr/eli/loi/2013/12/18/DEFX1317084L/jo#JORFARTI000028338886)

[43] https://exegetes.eu.org/dossiers/lpm/

[44] https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000029958091&dateTexte=&categorieLien=id

[45] https://exegetes.eu.org/dossiers/lpm.html

[46] Décret n°2011-219 du 25 février 2011 and article R. 10-13 du code des postes et communications électroniques (CPCE): https://exegetes.eu.org/dossiers/abrogationretention.html

[47] This information was compiled thanks to direct input from the Exégètes Amateurs (input from Lori Roussey on May 31 st , 2017).

[48] https://www.bna.com/data-residency-requirements-n57982069680/

[49] The information was compiled thanks to input from Professor Matthias Bäcker. See https://www.twobirds.com/en/news/articles/2017/germany/german-traffic-data-retention-law-considered-invalid ; https://www.justiz.nrw.de/nrwe/ovgs/vg_koeln/j2017/9_L_1009_16_Beschluss_20170125.html

[50] https://www.noerr.com/en/newsroom/News/data-retention-bundesnetzagentur-stops-enforcement-after-ruling-by-higher-administrative-court.aspx

[51] https://www.openrightsgroup.org/assets/files/legal/ORG_PI_Hungarian%20Constitutional%20Court%20submissions_final.pdf

[52] https://www.efa.org.au/2015/07/29/european-data-retention-laws-update/

[53] See https://edri.org/hungarian-data-retention-case-org-pi-and-scholars-file-amicus-briefs/ ; http://public.mkab.hu/dev/dontesek.nsf/0/8F2530FED210D050C1257DF8005DACEB?OpenDocument

[54] http://www.bakerinform.com/home/2016/7/15/hungary-introduces-new-surveillance-and-encryption-regulatons-affecting-online-communications

[55] http://www.statewatch.org/news/2017/mar/eu-council-datret-6726-REV-1-17.pdf

[56] https://www.openrightsgroup.org/assets/files/legal/Data_Retention_status_table_updated_April_2015_uploaded_finalwithadditions.pdf

[57] https://www.digitalrights.ie/dri-challenges-idependence-of-irelands-data-protection-commissioner/

[58] http://www.thejournal.ie/journalists-phones-3396896-May2017/

[59] The information was compiled through input from Digital Rights Ireland.

[60] http://www.statewatch.org/news/2017/mar/eu-council-datret-6726-REV-1-17.pdf

[61] Codice in materia di protezione dei dati personali, D.Lgs. 30/06/2003 n. 196 ("Codice Privacy") (Personal Data Protection Code, Legislative Decree no. 196, Section 132 (Traffic Data Retention for Other Purposes) (30 June 2003)).

[62] See https://edri.org/italy-plans-extend-telecoms-data-retention-increase-censorship-powers/

[63] Decreto-Legge 18 febbraio 2015, n. 7, supra note 5, at 4-bis

[64] Decreto-Legge 30 dicembre 2016, n. 244, Proroga e definizione di termini.

[65] For further reading, see The Data Retention Saga Continues: European Court of Justice and EU Member States Scrutinize National Data Retention Laws, Jones Day (August 2016), available at http://www.jonesday.com/the-data-retention-saga-continues-european-court-of-justice-and-eu-member-states-scrutinize-national-data-retention-laws-08-11-2016/

[66] For further reading see https://edri.org/italy-plans-extend-telecoms-data-retention-increase-censorship-powers/

[67] http://www.stibbe.com/en/news/2015/april/a-new-luxembourg-bill-on-data-retention

[68] Article 67-1 of the Criminal Code and Articles 5, 5-1 and 9 of the 2005 Privacy Act

[69] Article 5 of the Privacy Act 2005

[70] Article 9 of the Privacy Act 2005

[71] Article 67 -1 (4) of the Criminal Code contains an exhaustive list of offences. http://www.stibbe.com/en/news/2015/april/a-new-luxembourg-bill-on-data-retention

[72] CURRENT SITUATION TO BE CHECKED but see: http://europeanlawblog.eu/2016/07/25/the-future-of-national-data-retention-obligations-how-to-apply-digital-rights-ireland-at-national-level/

[73] Information obtained from Rejo Zenger at Bits of Freedom.

[74] Input received from Vincent Böhre at Privacy First, see https://www.privacyfirst.eu/focus-areas/law-and-politics/656-the-netherlands-under-the-united-nations-magnifying-glass.html

[75] Name of the law: Wijziging van de Telecommunicatiewet en het Wetboek van Strafvordering in verband met de bewaring van gegevens die zijn verwerkt in verband met het aanbieden van openbare telecommunicatiediensten en openbare telecommunicatienetwerken (aanpassing bewaarplicht telecommunicatiegegevens)

[76] For all parliamentary documents on the proposed Dutch data retention Bill, see https://zoek.officielebekendmakingen.nl/zoeken/resultaat/?_zkt=Uitgebreid&pst=ParlementaireDocumenten&dpr=Alle&spd=20170615&epd=20170615&dosnr=34537&kmr=EersteKamerderStatenGeneraal%7cTweedeKamerderStatenGeneraal_%7cVerenigdeVergaderingderStatenGeneraal&sdt=

[77] The actual list of types of data that is to be retained by telecom operators is defined in an addendum to the law: "Bijlage behorende bij artikel 13.2a van de Telecommunicatiewet"

[78] Information compiled thanks to input from Bits of Freedom and Privacy First.

[79] https://en.panoptykon.org/sites/default/files/Katarzyna_Szymielewicz_Data%20Retention%20in%20Poland_The%20Issue%20and%20the%20Fight.pdf#overlay-context_=

[80] http://www.liberties.eu/en/news/right-to-privacy-police-act-poland

[81] http://www.venice.coe.int/webforms/documents/?pdf=CDL-REF(2016)036-e

[82] https://nordvpn.com/blog/poland-surveillance-law/

[83] Information compiled thanks to input from Fundacja Panoptykon.

[84] http://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/nota_pratica_7_retencao_de_dados.pdf

[85] http://www.academia.edu/864352/Surveillance_and_Data_Protection_why_is_data_retention_regulation_so_relevant

[86] At least as of March 2017, see: http://www.statewatch.org/news/2017/mar/eu-council-datret-6726-REV-1-17.pdf

[87] Additional information was provided by Eduardo Santos, President of Associação D3 - Defesa dos Direitos Digitais. http://www.presidencia.pt/?idc=10&idi=134159

[88] See the Criminal Procedure Code at Article 152 http://legeaz.net/noul-cod-procedura-penala-ncpp/art-152

[89] https://www.juridice.ro/423743/obtinerea-datelor-generate-sau-prelucrate-de-catre-furnizorii-de-retele-publice-de-comunicatii-electronice-sau-furnizorii-de-servicii-de-comunicatii-electronice-destinate-publicului-si-retinute-de-cat.html

[90] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2951089

[91] Information compiled thanks to input from Association for Technology and Internet.

[92] http://www.eisionline.org/index.php/en/projekty-m-2/ochrana-sukromia/109-the-slovak-constitutional-court-cancelled-mass-surveillance-of-citizens

[93] http://www.eisionline.org/images/Data_retention_rozhodnutie_PL_US_10_2014.pdf

[94] Specifically, it proclaimed provisions § 58(5) to (7) and § 63(6) of the Electronic Communications Act (Act No. 351/2011 Coll.), which until now required mobile network providers to track the communication of their users, as well as provisions of § 116 of the Penal Code (Act No. 301/2005 Coll.) and § 76(3) of the Police Force Act (Act No. 171/1993 Coll.), which allowed access to this data, to be in contradiction to the constitutionally guaranteed rights of citizens to privacy and personal data.

[95] http://fra.europa.eu/en/theme/information-society-privacy-and-data-protection/data-retention

[96] Pursuant to §57(4) of law 351/2011

[97] See §57(5) of law 351/2011

[98] See §58(5)-(7) of law 351/2011

[99] The procedure is specified in §63 (5) - (8) of law 351/2011

[100] We have received input from Matej Gera at the European Information Society Institute.

[101] Act on Electronic Communications, ZEKom-1 articles 162, 163, 164, 165, 166, 167, 168 in 169.

[102] EDRI coverage: https://edri.org/slovenia-data-retention-unconstitutional/

[103] Constitutional Court judgement U-I-65/13-19 of 3 July 2014, available, only in Slovenian, here: https://www.ip-rs.si/fileadmin/user_upload/Pdf/sodbe/US_RS_ZEKom-1_3julij2014.tif

[104] Article 149.b of the Criminal Procedure Act

[105] Guidelines: https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/PIA_guideliness_for_introduction_of_new_police_powers_english.pdf

[106] http://www.statewatch.org/news/2017/mar/eu-council-datret-6726-REV-1-17.pdf

[107] The information dates from March 2017, see http://www.statewatch.org/news/2017/mar/eu-council-datret-6726-REV-1-17.pdf

[108] https://www.unodc.org/res/cld/document/svn/criminal_procedure_act_of_slovenia_html/Slovenia_CriminalProcedureAct2007.pdf

[109] Information compiled thanks to input from the Information Commissioner of the Republic of Slovenia dating from the 20 th of June 2017.

[110] https://observatory.mappingtheinternet.eu/page/data-retention-legislation-europe

[111] http://fra.europa.eu/en/theme/information-society-privacy-and-data-protection/data-retention

[112] http://www.lexology.com/library/detail.aspx?g=a886514b-71ab-4779-a2e7-d1486076e01b
https://www.efa.org.au/2015/07/29/european-data-retention-laws-update/

[113] https://www.boe.es/buscar/act.php?id=BOE-A-2014-4950

[114] https://www.twobirds.com/en/news/articles/2007/spain-new-law-retention-data-ecomms-public-comms-networks

[115] Information compiled thanks to input from the Alfa and Simona from the Spanish NGO Xnet, dating from the 5 th of July 2017. 116 http://www.statewatch.org/news/2017/mar/eu-council-datret-6726-REV-1-17.pdf

[116] http://www.statewatch.org/news/2017/mar/eu-council-datret-6726-REV-1-17.pdf
[117] Paras 16a, 16d, Lagen om elektronisk kommunikation (LEK) (Datalagringslagen)
[118] Tele 2 / Watson joined Cases C-203/15 and C-698/15 of 21 December 2016, at para 46
[119] Ibid at para 48
[120] Information received from Patrick Hiselius at Telia on 20 February 2017
[121] House of Lords, EU Committee, 3rd Report of Session 2017 - 19 'Brexit: the EU data protection package' https://publications.parliament.uk/pa/ld201719/ldselect/ldeucom/7/7.pdf