IS the mass collection of communications metadata legally equivalent to surveillance of the content of those communications? If so, does EU fundamental rights law have any bearing on its application? If it does, what is the appropriate relationship between the Court of Justice of the European Union and Member States' courts in balancing in the competing interests at stake? These questions came before a Grand Chamber of the CJEU in Joined Cases C-203/15 and C-698/15, *Tele2 Sverige AB v Post- och telestyrelsen* and *Secretary of State for the Home Department v Tom Watson and Others* ECLI:EU:C:2016:970 (*Watson*).

In a significant ruling, the CJEU held that domestic legislation permitting governments to require the indiscriminate retention of metadata by private communications providers is incompatible *per se* with the Charter of Fundamental Rights of the European Union ("CFR"). *Watson* is the third in a trilogy of data-protection cases, following the CJEU's earlier judgments in Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland v Minister for Communications, Marine and Natural Resources* [2014] E.C.R. I-238; [2014] 2 All E.R. (Comm) 1, and Case C-362/14, *Schrems v Data Protection Commissioner* EU:C:2015:650. In *Digital Rights Ireland*, the CJEU annulled Directive 2006/24/EC ("the Data Retention Directive" (OJ 2006 L 105/54)), which required communications providers to retain large amounts of metadata – including information sufficient to trace and identify the source and destination of a communication, and regarding the date, time and type of communications – though not the actual content of communications. This was found to constitute an unjustified interference with Articles 7 and 8 CFR (on respect for family and private life, and on the protection of personal data, respectively).

Following *Digital Rights Ireland*, the validity of domestic data retention regimes was in doubt. Two preliminary references were made to the CJEU as a result. The first, *Tele2 Sverige*, concerned a refusal by a Swedish communications provider to fulfil its obligations under the Swedish legislation that implemented the Data Retention Directive. When that refusal was challenged by the Swedish authorities, Tele2 brought proceedings in the administrative court. The referring court asked the CJEU whether indiscriminate retention of electronic communications data is "per se incompatible" with the Charter.

The second reference concerned the UK's Data Retention and Investigatory Powers Act 2014 ("DRIPA"). Under s. 1 of DRIPA, the Secretary of State had power to require communication providers to retain unlimited metadata for one of a number of specified public policy purposes. In judicial review proceedings before the Divisional Court, the legislation was declared incompatible with EU law. On the Government's appeal, the Court of Appeal referred two questions to the CJEU. The first asked

whether the decision in *Digital Rights Ireland* laid down mandatory requirements of EU law; the second asked whether the CFR provided any greater level of rights protection in this regard than the European Convention on Human Rights.

In answer to those questions, the CJEU held that national legislation providing for general and indiscriminate data retention is incompatible with Directive 2002/58 ("the e-Privacy Directive" (OJ 2002 L 201/37)), as read in light of the CFR. However, it remains open to Member States to make provision for targeted retention of data for the purpose of fighting serious crime, provided certain procedural safeguards are complied with. First, access of the national authorities to retained data must be subject to prior review by a court or independent administrative authority. Second, lawfully collected data must be retained within the European Union.

Watson is an important decision on the legal status of metadata. In both of the cases referred, the national legislation required the collection and retention of data relating to the identity and location of the user (such as their name, telephone number, and IP address), the identity of the recipient, and the date and time of the communication. The Court recognised that "[such] data, taken as a whole, is liable to allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as everyday habits, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them". Retreating from the distinction drawn in *Digital Rights Ireland* between metadata and the content of communications, the Court concluded that metadata could provide a "profile of the individuals concerned . . . that is no less sensitive, having regard to the right to privacy, than the actual content of communications". This was found to amount to a "particularly serious" interference with Articles 7 and 8 of the CFR, which could be justified only by the objective of fighting serious crime. Given the Court's recognition of these harms, it is surprising that it went on to endorse the potential use of geographical profiling by national surveillance authorities.

The CJEU's conclusion on mass metadata collection is, unsurprisingly, supported by privacy and human rights groups. The NGO Privacy International notes that profiles of this sort enable government agents to act on "erroneous correlations and unfair suppositions", sometimes provoked by structural biases, which can easily lead to the overt or covert discrimination against certain people or groups. Mass metadata collection can also have a "chilling effect", whereby the mere feeling of being watched causes citizens to limit their own freedom of expression.

More controversial is the CJEU's conclusion that general and indiscriminate retention will *always* "exceed the limits of what is strictly necessary" for the purposes of fighting serious crime. In this respect, the Court departed from the Advocate General's view that general retention measures

could sometimes be necessary, and that the national courts should be left to review their proportionality. In support of the latter approach, David Anderson Q.C., the UK's Independent Reviewer of Terrorism Legislation, notes (<https://terrorismlegislationreviewer.independent.gov.uk/cjeu-judgment-in-watson/> (21 December 2016)) that "because suspects are often not known in advance, data retention which is not universal in its scope is bound to be less effective as a crime reduction measure". Further, conspirators often "become more guarded in their use of communications as the moment of a crime approaches", making older data more useful than renewed surveillance.

Member States are now faced with the difficult task of limiting state surveillance, in line with the requirements laid down in *Watson*, without diminishing its usefulness. In the UK, it will be necessary to reassess the Investigatory Powers Act 2016 ("IPA"), which replaced DRIPA in December 2016. Much of DRIPA is replicated in the IPA regime: data can be retained and accessed on non-crime related grounds (s. 61(7)), bulk warrants can be issued (ss. 136, 158, 176), and prior independent review is not required in all cases (s. 76). The compatibility of the IPA with the CFR is therefore doubtful.

Even if the IPA survives unchallenged until after Brexit, *Watson* will exert a lasting impact, since the transfer of personal data to third countries is subject to certification that their data-protection standards are adequate. In *Schrems*, the CJEU held that third countries must ensure a level of protection of fundamental rights essentially equivalent to that guaranteed in the EU legal order. In the wake of the Snowden revelations about surveillance by the National Security Agency, it was held that data-protection standards in the US could not be presumed adequate. Following Brexit, the UK will surely seek to maintain an equivalent level of data protection. If it fails to do so, the transfer of personal data from Member States to the UK will constitute a breach of EU law.

Finally, EU constitutional lawyers will be most interested by the CJEU's approach in *Watson*, where the contested national legislation involved multiple competing interests. By establishing the balance of assertiveness and flexibility that should apply in such cases, the Court's response determines the reach of EU law into the legal orders of Member States. In this regard, though the substantive decision in *Watson* appears far-reaching, there are two reasons to consider the Court's approach more sensitive that it might immediately appear. First, the CJEU is rightly most confident in its development of EU fundamental rights law where, as here, there is no conflict with domestic constitutional requirements. This may explain why the Court, somewhat unusually, took the opportunity provided by the English Court of Appeal to compare the CFR with the European Convention on Human Rights ("ECHR"). The CJEU observed that Article 7 of the CFR "has no equivalent in the ECHR" and that Union law is not precluded

from "providing protection that is more extensive than the ECHR". It thereby re-affirmed the autonomy of EU fundamental rights law.

Secondly, the Court's jurisprudence in this field has developed not by diktat but through dialogue. *Watson* was decided in the wake both of the CJEU's two previous judgments on data protection, and of a number of national decisions annulling domestic data retention measures. This enabled the CJEU to construct a Community standard from an emergent national consensus. This reflects a process that Sabel and Gerstenberg ((2010) 16:5 E.L.J. 511, 550) have called "proceduralist" constitutionalism, by which the CJEU develops EU law by simultaneously reacting to Member States' constitutional orders and shaping a mutual accord. In its trilogy of data retention decisions – *Digital Rights Ireland*, *Schrems* and *Watson* – the Court has sought to forge a liberal consensus with individual privacy at its core. It remains to be seen how the Member States will respond.

Isabella Buono and Aaron Taylor

Address for Correspondence: Email: Isabella.Buono@cantab.net; St Edmund's College, Cambridge CB3 0BN, UK. Email: almt3@cam.ac.uk

CONFIDENTIALITY AND PUBLIC AUTHORITIES: FUNDAMENTAL RIGHTS, LEGALITY AND DISCLOSURE FOR STATUTORY FUNCTIONS

TAXPAYER confidentiality has a long history of protection in the UK. It is a fundamental part of the tax system. It has been considered invaluable by the executive for the efficient collection of taxation, protected by Parliament since the Income Tax Act 1799 and recognised by the courts as a "vital element in the working of the system" (*Inland Revenue Commissioners v National Federation of Self-Employed and Small Businesses Ltd.* [1982] A.C. 617, 633, per Lord Wilberforce).

Historically, the justification for imposing taxpayer confidentiality was robustly State-centric: confidentiality encourages detailed taxpayer disclosure of highly sensitive information, which enables the tax yield to be greater than would otherwise be the case. The Supreme Court considered the scope of taxpayer confidentiality in *R. (Ingenious Media) v Commissioners for Her Majesty's Revenue and Customs* [2016] UKSC 54; [2016] 1 W.L.R. 4164 and favoured quite a different rationale, holding that confidentiality was a common-law fundamental right of taxpayers, with the effect that the power of HM Revenue and Customs ("HMRC") to disclose information was curtailed in circumstances where HMRC reasonably considered disclosure would ultimately help it to increase the tax yield.

The leading judgment of Lord Toulson is interesting and important for two reasons as part of a re-emerging trend to recognise fundamental rights in the common law. First, the reasoning of the Supreme Court suggests a