

Maurer School of Law: Indiana University

Digital Repository @ Maurer Law

Articles by Maurer Faculty

Faculty Scholarship

2018

An Unstoppable Force and an Immoveable Object? EU Data Protection Law and National Security

Fred H. Cate

Indiana University Maurer School of Law, fcate@indiana.edu

Christopher Kuner

Vrije Universiteit Brussel, Brussels

Orla Lynskey

London School of Economics

Christopher Millard


Queen Mary University

Nora Ni Loideain

University of London

Follow this and additional works at: <https://www.repository.law.indiana.edu/facpub>

See next page for additional authors

 Part of the [Information Security Commons](#), [National Security Law Commons](#), and the [Privacy Law Commons](#)

Recommended Citation

Cate, Fred H.; Kuner, Christopher; Lynskey, Orla; Millard, Christopher; Ni Loideain, Nora; and Svantesson, Dan Jerker B., "An Unstoppable Force and an Immoveable Object? EU Data Protection Law and National Security" (2018). *Articles by Maurer Faculty*. 2692.

<https://www.repository.law.indiana.edu/facpub/2692>

This Editorial is brought to you for free and open access by the Faculty Scholarship at Digital Repository @ Maurer Law. It has been accepted for inclusion in Articles by Maurer Faculty by an authorized administrator of Digital Repository @ Maurer Law. For more information, please contact rvaughan@indiana.edu.



LAW LIBRARY
INDIANA UNIVERSITY
Maurer School of Law
Bloomington

Authors

Fred H. Cate, Christopher Kuner, Orla Lynskey, Christopher Millard, Nora Ni Loideain, and Dan Jerker B. Svantesson

Editorial

An unstoppable force and an immovable object? EU data protection law and national security

Christopher Kuner*, Fred Cate**, Orla Lynskey**,
Christopher Millard**, Nora Ni Loideain** and Dan Svantesson**

The Grand Chamber of the Court of Justice of the European Union (EU) (CJEU/Luxembourg Court), the EU's highest court, is gaining a reputation for its more purposive and expansive interpretation and application of EU data protection law. This is particularly so in relation to the right to data protection, as guaranteed by Article 8 of the EU Charter of Fundamental Rights (EU CFR) which became part of EU law in 2009 following the entering into force of the Lisbon Treaty [Treaty on the Functioning of the EU (TFEU)].

In addition to Article 8 EU CFR, another important reform of EU data protection law in 2009 was Article 16 TFEU which provides an explicit legal basis for data protection legislation. Consequently, this relatively new legal framework (especially Article 8 EU CFR) has played an instrumental role in a succession of landmark judgments concerning the requirements and minimum safeguards that must be applied by EU Member States when personal data is processed for the purposes of law enforcement and public security, or even national security with respect to third countries (non-EU states). One such new requirement is the need to provide that personal data is retained in the EU in order to ensure that it is subject to the independent supervision of EU data protection authorities. In its 2014 judgment of *Digital Rights Ireland*, the CJEU determined that this is 'an essential component' for the protection of individuals under EU data protection law.

Notwithstanding the apparently unstoppable force of the expanding scope of EU data protection law, EU law [Article 4(2) of the Treaty of the EU (TEU)] states that the EU

shall respect the equality of Member States before the Treaties as well as their national identities, inherent in their fundamental structures, political and constitutional,

inclusive of regional and local self-government. It shall respect their essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. In particular, national security remains the sole responsibility of each Member State.

Notably, Article 4 TEU clearly stresses that 'national security remains the sole responsibility of each Member State'. Hence, this exemption from EU law should mean that Article 8 EU CFR and Article 16 TFEU should not apply to any national security matters governed by domestic law as these provisions are only relevant to 'Member States when carrying out activities that fall within the scope of EU law.'

Soon after these major legal changes within EU law (particularly the elevation of data protection to a fundamental right) the Snowden revelations concerning systematic government surveillance, in the US and beyond, began to emerge. As we have discussed previously, exposure of these national security programmes has since led to soul-searching by policymakers worldwide about both the relevance and the effectiveness of existing legal frameworks for ensuring the adequate protection and security of privacy and personal data.¹ In particular, these revelations have cast a rather stark light on the extent to which legislators and courts have deferred to a State's interpretation of the situations it faces in permitting limitations on the rights of individuals where matters of national security arise given the sensitive and confidential nature of the information collected, analysed, and shared. Of course, at the EU level, as noted above, any fundamental rights-based scrutiny of Member State law governing national security has been deemed to fall outside of the competence of the CJEU.

* Editor-in-Chief.

** Editor.

1 See our Editorial on 'PRISM and Privacy: Will This Change Everything?' (2013) 3(4) International Data Privacy Law 217 <<http://idpl.oxfordjournals.org/content/3/4/217.full.pdf+html?sid=b7d189ef-0ab1-4b92-8dd9-dbaa2b4b024f>>.

A pending preliminary reference, however, to that court may shortly determine otherwise for an area of law and policymaking that has long been an immovable object of national sovereignty from the primacy of EU law.

The case at issue is one in a series of legal challenges brought by Privacy International, a leading international civil society organization based in the UK, against the Secretary of State for Foreign and Commonwealth Affairs and other public authorities regarding their respective powers concerning covert surveillance. The preliminary reference was submitted to the CJEU in October 2017. Responsibility for this referral lies with the UK Investigatory Powers Tribunal (IPT) which investigates complaints concerning the surveillance programmes of the UK's security and intelligence agencies.² Essentially, the IPT has been put in a position whereby it must seek clarification from the CJEU regarding whether or not, or to what extent, the privacy and data protection requirements and minimum safeguards established by the CJEU in its earlier judgments of *Digital Rights Ireland* and *Tele2 Sverige AB & Watson* apply in the context of national security. EU law provides that national courts of Member States are unable to rule on the validity of EU law and, therefore, must refer such cases to the CJEU.³

More specifically, the IPT has requested that the CJEU establish (especially in light of Article 4 TEU), whether the activities of the intelligence services in relation to the bulk acquisition and use of communications data (otherwise known as metadata) for the purposes of national security fall within the scope of EU law. Communications data does not reveal the content of a communication. Instead, it identifies the 'who', 'when', 'where', and 'how' of a communication. It may reveal much more about an individual's private life when done so in 'bulk'.

This latter method of monitoring may encompass the communications from all of an individual's devices (smartphones, tablets, and laptops). These may then be retained over a lengthy period of time (usually six months),⁴ combined, and analysed. The capacity to aggregate and sift through the resulting detailed profiles can be achieved through the combination of many isolated items of information that may not in themselves be considered private or personal. Hence, the bulk collection of communications data can provide very detailed 'narrative data' about an individual's public and private life, eg the nature of a relationship between

parties based on the frequency/time of their communications. Such information could prove to be valuable within a national security context with respect to identifying and tracking international networks of organized crime and terrorist groups and the detection of cyberattacks.

But what of the seemingly unequivocal clarity provided for by Article 4 TEU with respect to national security remaining the sole responsibility of Member States? What jurisprudential Gordian knot has prompted this preliminary reference? The answer lies with the CJEU's 2016 judgment of *Tele2 Sverige AB & Watson* and when it made legal history in the 2014 landmark decision of *Digital Rights Ireland*.

The proceedings in *Digital Rights Ireland* occurred during the height of the Snowden revelations and this may have influenced the outcome of the case. In any event, it culminated in the first striking down of an entire EU law for its incompatibility with the EU CFR. Previously, the impugned legislative instrument in question (the Data Retention Directive 2006/24/EC) had imposed a mandatory obligation on every EU Member State to ensure the mass retention of communications data (metadata) for the purpose of countering serious crime. Consequently, the fundamental rights requirements and safeguards established by the CJEU in *Digital Rights Ireland* posed a number of thorny questions for policymakers. The most significant of these questions was whether the CJEU had in fact held that the very measure of 'general and indiscriminate' retention of communications data itself was incompatible with EU fundamental rights, thereby rendering such surveillance invalid under EU law.

In contrast to the arguments of the European Commission and the Opinion of the Advocate General, the CJEU answered this question affirmatively in *Tele2 Sverige AB & Watson*. Furthermore, the Grand Chamber also established that in order to be compatible with EU law, national laws on data retention must be based on objective evidence making it possible to 'identify a public whose data is likely to reveal a link' with serious criminal offences and that that data contributes 'to fighting serious crime' or to 'preventing a serious risk to public security' (para 111). Does the latter term of 'public security' also cover all matters of national security? Certain parts of the CJEU's analysis in *Watson* suggest that the Luxembourg Court has in made this determination with respect to its

2 For all documents relating to this preliminary reference, see the IPT website <<http://www.ipt-uk.com/judgments.asp?id=41>>.

3 Case C-314/85 *Foto-Frost v Hauptzollamt Lübeck-Ost* [1987] ECR 4199.

4 Note that US law, under s 215 of the USA PATRIOT Act (since repealed following the Snowden revelations, replaced by new provisions under the USA Freedom Act), provided for the bulk retention of communications data by the NSA for up to five years.

interpretation of Article 15 of the e-Privacy Directive 2002/58/EC.

Article 15 provides that Member States can restrict the scope of traditional data protection safeguards and adopt legislative measures for the long-term retention of communications data. Such a restriction can be adopted if it 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’. Hence, Article 15(1) allows Member States to adopt legislation permitting data processing that would otherwise not be permitted under the e-Privacy Directive for certain legitimate purposes, including the bulk collection of communications data in the context of national security. Furthermore, Article 1(3) of the e-Privacy Directive also states that it does not apply to activities which fall outside of EU law and ‘in any case to activities concerning public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law’.

Rather than clearly limit its examination of the application of the e-Privacy Directive to data retention in the context of serious crime, the CJEU left open the question of whether data retention for all the legislative measures provided under Article 15(1) must comply with the requirements and safeguards established in *Watson*. The CJEU’s reasoning for this determination was based on the Luxembourg Court ‘having regard to the general structure of Directive 2002/58’, and that to hold otherwise would leave Article 15 ‘deprived of any purpose’. As a result, the CJEU is now being asked to confirm whether in fact the discretion of Member States to permit limitations on the data protection rights of individuals where matters of national security arise remains the sole responsibility of Member States, or whether these restrictions are now subject to EU law, and thus the scrutiny and review of the CJEU.

There are significant concerns regarding the often uncertain and vague reasoning provided in *Watson* and in other recent landmark data privacy judgments. In

particular, the analysis and application of the legality, necessity, and proportionality requirements that apply to the qualified rights of respect for private life and data protection under the EU CFR are very general in scope. Article 52 EU CFR provides that these rights are not absolute and must be balanced with other legitimate competing interests, such as law enforcement and national security. Significantly in *Watson*, the relevant jurisprudence lacks any assessment of how the risks posed by the retention of communications data differ from the risks involved in the subsequent use of the data. In other words, the everyday capture and storage of such data is ‘qualitatively different’ from the use of that data to determine whether or not an individual is, or is not, a terrorist threat.⁵ In addition, there is little detailed examination of the different ways in which an interference with the fundamental rights to private life and data protection will warrant the consideration and weighting of different factors depending on the legitimate purpose at issue (law enforcement versus national security).

Going forward, a more careful approach is needed in order to provide for the development of a more consistent, clear, and robust fundamental rights framework with respect to the proportionately of the limitations that are placed on an individual’s rights to private life, and data protection. The quality of legal reasoning in the CJEU could also benefit from acknowledgement of the traditionally more comprehensive, and consequently more robust, precedents in the case law of the European Court of Human Rights and in deciding whether there is a need to follow or distinguish its approach from this more experienced supranational court. This clarity in reasoning could greatly assist policymakers, supervisory authorities, and courts, at both the EU and domestic level and beyond, in the future development, implementation and review of legislation concerning data protection and wide-scale data processing for national security. In any event, this is likely to remain one of the most dynamic and technically complex areas of privacy and data protection law.

doi:10.1093/idpl/ipy003

5 CJ Bennett, *The Privacy Advocates* (MIT Press, Massachusetts 2008) 17.