

ARTICLE

The Right to Privacy—A Fundamental Right in Search of Its Identity: Uncovering the CJEU’s Flawed Concept of the Right to Privacy

Valentin M. Pfisterer*

(Received 22 March 2018; accepted 25 July 2018)

Abstract

In recent years, the CJEU has impressively brought to bear the protection of the fundamental rights to privacy and protection of personal data as contained in the CFREU. The Court’s decisions in the *Digital Rights*, *Schrems*, *Tele2*, and *PNR* cases have reshaped the political and legal landscape in Europe and beyond. By restricting the powers of the governments of EU Member States and annulling legislative acts enacted by the EU legislator, the decisions had, and continue to have, effects well beyond the respective individual cases. Despite their strong impact on privacy and data protection across Europe, however, these landmark decisions reveal a number of flaws and inconsistencies in the conceptualization of the rights to privacy and protection of personal data as endorsed and interpreted by the CJEU. This Article identifies and discusses some of the shortcomings revealed in the recent CJEU privacy and data protection landmark decisions and proposes to the CJEU a strategy aimed at resolving these shortcomings going forward.

Keywords Privacy; data protection; Charter of Fundamental Rights of the European Union; Court of Justice of the European Union

A. Privacy on the Rise

Privacy is on the rise. This contention does not refer to the overall development in Western societies in which the private realm is largely felt to be losing ground to the public realm due to the use of increasingly sophisticated surveillance by governments and the proliferation of ever more intrusive data processing technologies offered and applied by mammoth technology companies. It rather refers to the jurisprudence of the Court of Justice of the European Union (“CJEU” or “Court”) in matters of privacy and data protection, as inspired by the European Court of Human Rights (“ECtHR”). In recent years, the CJEU has relentlessly strengthened the protection of the fundamental rights to privacy and protection of personal data as contained in the Charter of Fundamental Rights of the European Union (“CFREU”).¹ The Court has, *inter alia*, (1) found the proposed agreement between Canada and the EU on the transfer and processing of passenger name record (“PNR”) data partly incompatible with the rights to privacy and protection of personal data (*PNR* case);² (2) reduced the discretion of EU Member States to derogate from the statutory protection of personal data in electronic communications by virtue of

*Dr. Valentin M. Pfisterer is an attorney in Frankfurt am Main with an LL.M. from New York University School of Law and a PhD in law from University of Leipzig.

¹Valentin Pfisterer, *Finanzprivatsphäre in Europa*, EuR EUROPARECHT 2016, 553–554.

²CJEU, *PNR* Opinion 1/15, ECLI:EU:C:2017:592, Judgement of 26 July 2017.

the requirements enshrined in the rights to privacy and protection of personal data (*Tele2 case*);³ (3) struck down the so-called Safe Harbor Principles which allowed for the transatlantic transfer of personal data based on their incompatibility with the rights to privacy and protection of personal data (*Schrems case*);⁴ and (4) invalidated the Data Retention Directive of 2006 as violating the rights to privacy and protection of personal data (*Digital Rights case*)⁵—all this within only a few years.⁶

With its decisions in the *Digital Rights*, *Schrems*, *Tele2*, and *PNR* cases, the CJEU “rocked” the political and legal landscape in Europe and beyond. These decisions had, and continue to have, far-reaching effects, as they restrict the powers of the governments of EU Member States and set aside legislative acts enacted by the EU legislator. The decision of the CJEU in the *Schrems* case, for example, resulted in enormous unrest on the part of businesses on both sides of the Atlantic that were afraid that the cross-border transfers of personal data between the EU and the U.S.—as usually carried out by them—had to be stopped immediately.⁷ Hectic political tug-of-war between the leaderships of the U.S. and the EU ensued with the purpose of establishing a new legal basis for transatlantic transfers of personal data as quickly as possible that is both acceptable to the international business community and compliant with the CFREU. These efforts resulted in the recent enactment of the Privacy Shield, a successor instrument to the Safe Harbor Principles.⁸

The enormous practical impact of the aforementioned landmark decisions appears to be inversely proportionate to the rigor and clarity of the CJEU’s conceptualization of the rights to privacy and protection of personal data, on which the cases are based. In other words, these decisions reveal a number of shortcomings in the conception of the relevant fundamental rights as endorsed and brought to bear by the CJEU. Also, other less well-known decisions in matters of privacy and data protection handed down by the CJEU around the time of and after these decisions have, as far as can be seen, not resolved, or significantly contributed to the resolution of, these conceptual shortcomings.⁹

In this Article, I identify and discuss some conceptual flaws and inconsistencies revealed in the recent CJEU privacy and data protection landmark decisions and propose to the CJEU a strategy aimed at resolving these shortcomings going forward. For this purpose, I first summarize these

³CJEU, Case C-203/15, *Tele2 Sverige AB v. Post-och Telestyrelsen*, ECLI:EU:C:2016:970, Judgement of 21 Dec. 2016.

⁴CJEU, Case C362/14, *Schrems v. Data Protection Comm’r*, ECLI:EU:C:2015:650, Judgement of 6 Oct. 2015.

⁵CJEU, Joined Cases C293/12 & C594/12, *Dig. Rts. Ir. v. Minister for Comm.*, ECLI:EU:C:2014:238, Judgement of 8 Apr. 2014 [hereinafter *Digital Rights*].

⁶See JÖRG TERHECHTE, *KONSTITUTIONALISIERUNG UND NORMATIVITÄT DER EUROPÄISCHEN GRUNDRECHTE*, 89 (2011) (discussing the notion of the CJEU as a “fundamental rights court”); Jürgen Kühling, *Der Fall der Vorratsdatenspeicherungsrichtlinie und der Aufstieg des EuGH zum Grundrechtsgericht*, NVwZ 681–85 (2014).

⁷See generally Richard Epstein, *Europe’s top court goes off the rails*, POLITICO, (October 8, 2015), <https://www.politico.eu/article/CJEU-off-the-rails-safe-harbor-eu-us-data-protection>; Richard Epstein, *The ECJ’s Fatal Imbalance: Its cavalier treatment of national security issues poses serious risk to public safety and sound commercial practices*, 12 EUR. CONST. L. REV. 330 (2016) (criticizing the disregard by the CJEU of the reliance interests of the business community); Christopher Kuner, *The Sinking of the Safe Harbor*, VERFASSUNGSBLOG (Oct. 8, 2015), <http://verfassungsblog.de/the-sinking-of-the-safe-harbor-2> (same).

⁸See Commission implementing decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, 2016 O.J. (L 207) 1; see generally Martin Weiss & Kristian Archick, *U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield*, CONG. RES. SERV. 8 (May 19, 2016) (providing a U.S. perspective); David Bender, *Having mishandled Safe Harbor, will the CJEU do better with Privacy Shield? A US perspective*, 6 INT’L DATA PRIVACY 117 (2016); see generally Thilo Weichert, *EU-US-Privacy-Shield—Ist der transatlantische Datentransfer nun grundrechtskonform? Eine erste Bestandsaufnahme*, ZEITSCHRIFT FÜR DATENSCHUTZ 209 (2016) (providing a European perspective).

⁹See e.g., CJEU, Case C-165/14, *Marin v. Administración del Estado*, ECLI:EU:C:2016:675, Judgement of 13 Sept. 2016, at 66, 81; CJEU, Case C-304/14, *Sec’y of State for the Home Dep’t v. CS*, ECLI:EU:C:2016:674, Judgement of 13 Sept. 2016, at 36, 48; CJEU, Case C-438/14, *Wolfferdorff v. Standesamt der Stadt Karlsruhe*, ECLI:EU:C:2016:401, Judgement of 2 June 2016, at 35, 54; CJEU, Case C-582/14, *Breyer v. Bundesrepublik Deutschland*, ECLI:EU:C:2016:339, Judgement of 19 Oct. 2016; CJEU, Case C-558/14, *Khachab v. Subdelegación del Gobierno en Álava*, ECLI:EU:C:2016:285, Judgement of 21 Apr. 2016, at 27.

decisions to the extent relevant for the purpose stated above in Part B; second, I discuss the shortcomings identified and how they might be resolved in Part C; and finally, I summarize my thoughts and arguments and propose to the CJEU a strategy for the way forward in Part D.

B. From *Digital Rights* to *PNR*—the Recent CJEU Landmark Decisions in the Area of Privacy and Data Protection

By virtue of their far-reaching practical impact, the CJEU decisions in the *Digital Rights*, *Schrems*, *Tele2*, and *PNR* cases have become, and are considered as, landmark decisions in the area of privacy and data protection. In this section, I will briefly summarize these cases to the extent relevant for the discussion to follow.

I. *Digital Rights*—*Mass Data Retention on Trial*

In the *Digital Rights* case from 2014,¹⁰ *Digital Rights Ireland Ltd.*, an Irish privacy rights activist organization, challenged the validity of the Data Retention Directive of 2006. The Directive¹¹ imposed the obligation on providers of electronic communication services to retain traffic and location data relating to the users of such services and granted to national law enforcement authorities the right to access such data for the purpose of investigation, detection, and prosecution of serious crimes. *Digital Rights Ireland Ltd.* argued, *inter alia*, that both the retention obligation and the access rights violated the rights to privacy and protection of personal data of the users as enshrined in the CFREU. In its decision, the Court found the retention obligation, as well as the access rights, to constitute a violation of the rights to privacy and protection of personal data and, as a consequence, declared the Data Retention Directive invalid.¹²

II. *Schrems*—*Challenging Transatlantic Data Transfers*

In the *Schrems* case from 2015¹³, Maximilian Schrems, an Austrian privacy rights activist, challenged the validity of the so-called Safe Harbor Principles or, more precisely, the Commission Decision acknowledging these principles¹⁴ based on the—now repealed—Data Protection Directive.¹⁵ The Data Protection Directive generally prohibited the transfer of personal data from within the EU to recipients located outside of the EU. By way of exemption, however,

¹⁰*Digital Rights*, Joined Cases C293/12 & C594/12, *supra* note 5; see generally Marie-Pierre Granger & Kristina Irion, *The Court of Justice and the Data Retention Directive in Digital Rights Ireland: Telling off the EU Legislator and Teaching a Lesson in Privacy and Data Protection*, 39 EUR. L. REV. 835 (2014); Orla Lynskey, *The Data Retention Directive is Incompatible with the Rights to Privacy and Data Protection and is Invalid in its Entirety: Digital Rights Ireland*, 51 COMMON MKT. L. REV. 1789 (2014); Kühling, *supra* note 6, at 681–85.

¹¹Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC, 2006 O.J. (L 105) 54 [hereinafter *Data Retention Directive*].

¹²*Digital Rights*, Joined Cases C293/12 & C594/12, *supra* note 5, at 73.

¹³*Schrems*, Case C362/14, *supra* note 4; see generally Christina Lam, *Unsafe Harbor: The European Union's Demand for Heightened Data Privacy Standards in Schrems v. Irish Data Protection Commissioner*, 40 B.C. INT. AND COMP. L. REV. 1 (2017).

¹⁴Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the Safe Harbour Privacy Principles and Related Frequently Asked Questions Issued by the US Department of Commerce, 2000 O.J. (L 215) 7 [hereinafter *Commission Decision 2000/520/EC*].

¹⁵Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995 O.J. (L 281) 31 [hereinafter *Data Protection Directive*]; see also Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC, 2016 O.J. (L 119) 1 (replacing the *Data Protection Directive*).

such transfer was permissible if the Commission found that the relevant third country ensured an “adequate level of [data] protection. ...”¹⁶ In relation to the United States, the Commission found the level of data protection adequate to the extent that the relevant data recipients self-certified under the Safe Harbor Principles agreed upon between the Commission and the U.S. Government.¹⁷ Schrems, a user of the social network Facebook, challenged the data transfers on the basis of the Safe Harbor Principles from Facebook Ireland Ltd.—which generated personal data from Facebook users in Europe—to its U.S.-based parent company, Facebook, Inc. He argued, *inter alia*, that—in view of the large-scale and generalized surveillance measures applied by U.S. intelligence services—the data protection level guaranteed in the United States was not adequate within the meaning of the Data Protection Directive. In its decision, the CJEU found the Commission Decision incompatible with the requirements of the Data Protection Directive, as interpreted in accordance with Articles 7 and 8 CFREU, and consequently annulled the Decision.¹⁸

III. *Tele2—Limiting EU Member States’ Authority to Derogate from Data Protection*

In the *Tele2* case from 2016¹⁹, *Tele2 Sverige AB*, a Swedish electronic communications services provider, challenged the validity of Swedish national legislation—enacted based on Article 15(1) of the Directive on Privacy and Electronic Communications—imposing far-reaching retention obligations on electronic communications services providers. The purpose of the Directive²⁰ is to harmonize the national laws on data protection in connection with the processing of personal data in electronic communications. The Directive contains a general rule whereby traffic and location data generated in connection with the transmission of communication must be deleted or anonymized after the completion of the transmission. In derogation from that general rule, Article 15(1) of the Directive allows national legislators to enact provisions restricting the obligation to delete or anonymize such data, or even requiring the retention of certain data. *Tele2 Sverige AB* argued that, in view of the *Digital Rights* decision of the CJEU (see above), this exemption must be considered void based on its alleged violation of Articles 7 and 8 CFREU. In its decision, the CJEU held that Article 15(1) of the Directive, read in the light of Articles 7 and 8 CFREU, must be interpreted so as to preclude a data retention obligation as the one entailed in the Swedish national legislation.²¹

IV. *PNR—Challenging Transatlantic Data Transfers, Once Again*

Finally, in the *PNR* case from 2017,²² the European Parliament requested an opinion from the CJEU on whether the proposed agreement between Canada and the EU on the transfer and processing of PNR data was compatible with, *inter alia*, Articles 7 and 8 CFREU. The proposed PNR agreement provided for the transfer by air carriers servicing between the EU and Canada of

¹⁶See Data Protection Directive *supra* note 15, art. 25(6).

¹⁷Commission Decision 2000/520/EC, *supra* note 14.

¹⁸Schrems, Case C362/14, *supra* note 4, para 106–07.

¹⁹*Tele2 Sverige AB*, Case C-203/15, *supra* note 3; see generally Iain Cameron, *Balancing Data Protection and Law Enforcement Needs: Tele2 Sverige and Watson*, 54 COMMON MKT. L. REV. 1467 (2017); Isabella Buono & Aaron Taylor, *Mass Surveillance in the CJEU: Forging a European Consensus*, CAMBRIDGE L.J. 250 (2017).

²⁰Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on privacy and electronic communications), 2002 O.J. (L 201) 37.

²¹*Tele2 Sverige AB*, Case C-203/15, *supra* note 3, para. 134.

²²PNR Opinion 1/15, *supra* note 2; see generally Elena Carpanelli & Nicole Lazzarini, *PNR: Passenger Name Record, Problems not Solved? The EU PNR Conundrum after Opinion 1/15 of the CJEU*, 42 AIR & SPACE L. 377 (2017); Hielke Hijmans, *PNR Agreement EU-Canada Scrutinised: CJEU Gives Very Precise Guidance to Negotiators*, 3 EUR. DATA PROT. L. REV. 406 (2017).

certain personal data of travelers to the Canadian government for the purpose of combatting serious crime and terrorism. In its opinion, the CJEU concluded that the proposed PNR agreement was, in certain respects, incompatible with the rights to privacy and protection of personal data.²³

C. Inconsistencies and Truisms—Shortcomings in the Recent Privacy Jurisprudence of the CJEU

The above summaries of the recent landmark decisions of the CJEU in the area of privacy and data protection allow us to proceed to discuss the shortcomings in the conception of the fundamental rights to privacy and protection of personal data as endorsed and brought to bear by the CJEU. These shortcomings relate to: the relationship between the rights to privacy and protection of personal data; the eligible beneficiaries of the right to privacy; the particular importance of the right to privacy; the function of the right to privacy in society; and, ultimately, the essence of the right to privacy.

I. Privacy and Data Protection—or: Privacy or Data Protection? On the Relationship Between the Right to Privacy and the Right to Protection of Personal Data

Seventeen years after the proclamation of the CFREU, the relationship between the right to privacy—Article 7 CFREU—and the right to protection of personal data—Article 8 CFREU—is still unclear. The recent landmark decisions contribute to the “longstanding confusion about the distinction between the right to data protection and privacy.”²⁴

In the *Digital Rights* and *PNR* cases, the CJEU analyzed the interference by the relevant measures with the right to privacy and the right to protection of personal data in a strictly separated fashion.²⁵ In doing so, the Court appears to suggest that the two guarantees constitute two separate fundamental rights—each one of them complete in itself. Even more clearly, the Court expressly stated in the *Tele2* case that “Article 8 of the Charter concerns a fundamental right which is distinct from that enshrined in Article 7 of the Charter and which has no equivalent in the ECHR.”²⁶

In contrast, the Court stressed in the *Digital Rights* case “the important role played by the protection of personal data in the light of the fundamental right to respect for private life. . . .”²⁷ In its decision in the *Promusicae* case from 2008, the Court similarly labeled the fundamental right of Article 8 CFREU as “the right that guarantees protection of personal data and hence of private life.”²⁸ These statements may be understood to suggest that the right to protection of personal data is a fraction of, and potentially inferior or functional to, the right to privacy.

Ultimately, in the *Schrems* and *Tele2* cases—and in contrast to the approach taken in the *Digital Rights* and *PNR* cases—the Court merged its analysis of the interference of the relevant measures with the right to privacy and the right to protection of personal data in a way that disallows the reader to discern the criteria governing, or relevant to, each one of the rights and how they unfold in the case at hand.²⁹ To make the confusion even more pronounced, the Court mentioned in the *Schecke* case from 2010 a “right to respect for private life with regard

²³PNR Opinion 1/15, *supra* note 2, para. 232.

²⁴Christopher Kuner, *Reality and Illusion in EU Data Transfer Regulation Post Schrems*, 18 GERMAN L.J. 881, 892 (2017).

²⁵See *Digital Rights*, Joined Cases C293/12 & C594/12, *supra* note 5, para. 32–37; *PNR* Opinion 1/15, *supra* note 2, para. 122–26.

²⁶*Tele2 Sverige AB*, Case C-203/15, *supra* note 3, para. 129 (emphasis added).

²⁷*Digital Rights*, Joined Cases C293/12 & C594/12, *supra* note 5, para. 48.

²⁸See CJEU, Case C-275/06, *Promusicae v. Telefónica de España SAU*, ECLI:EU:C:2008:54, Judgement of 29 Jan. 2008, at para. 63 (emphasis added).

²⁹See *Schrems*, Case C362/14, *supra* note 4, para. 91–92; *Tele2 Sverige AB*, Case C-203/15, *supra* note 3, para. 92.

to the processing of personal data, recognised by Articles 7 and 8 of the Charter.”³⁰ The approach taken by the CJEU in the in the *Schrems* and *Tele2* cases, and the notion introduced by the CJEU in the *Schecke* case, may be understood to suggest that there is one combined, uniform right to respect for private life with regard to the processing of personal data—potentially in addition to the individual rights under Articles 7 and 8 CFREU.

For the purpose of untying the Gordian knot, the right to privacy and the right to protection of personal data should be understood as two separate fundamental rights, as expressly stated by the CJEU in the *Tele2* case.³¹

First, the guarantees are laid down in two separate provisions in the CFREU. The right to privacy in Article 7 CFREU was modeled by the Convention which drafted the CFREU after the right to privacy in Article 8 ECHR, mirroring its quartet of protections in relation to the notions of private life, family life, home, and communications or correspondence.³² The right to protection of personal data in Article 8(1) CFREU was newly introduced by the Lisbon Treaty—with no equivalent in the ECHR.³³ It is true that in the past—including after the proclamation of the CFREU—the CJEU used the right to privacy—as opposed to the right to protection of personal data—for the purpose of guaranteeing the protection of personal data and in doing so, relied on and made reference to Article 8 ECHR.³⁴ Indeed, and as confirmed by Article 6(3) of the Treaty on the European Union, the fundamental rights entailed in the ECHR—such as the right to privacy in Article 8 ECHR—constitute general principles of EU law.³⁵ Absent an accession by the EU to the ECHR, however, the ECHR has not been formally incorporated into EU law.³⁶ Therefore, since the adoption of the Lisbon Treaty, the protection of personal data should—in the realm of EU law—be guaranteed by the right specifically designed for this purpose: The right to protection of personal data as contained in Article 8(1) CFREU.³⁷

Second, the right to privacy or, more specifically, the right to respect for private life, is part of a quartet consisting of—in addition to private life—family life, home, and communications (see above). In contrast, the right to protection of personal data is set forth in a separate article. Also, in addition to establishing the basic guarantee of protection of personal data,³⁸ that article also contains a detailed, programmatic dimension in its second paragraph, explicitly requiring that personal data be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Further, it establishes that compliance with these rules shall be subject to control by an independent authority.³⁹ Therefore, the substantive delineation of the guarantees, the respective history and context of their creation, and the mindset and program speaking from their respective wording are different and distinct.

Third, and most importantly, the essence of the right to privacy and the essence of the right to protection of personal data are different—as acknowledged by the CJEU in the *Digital Rights*

³⁰CJEU, Joined Cases C92/09 & C93/09, *Schecke v. Land Hessen*, ECLI:EU:C:2010:662, Judgement of 9 Nov. 2010, at para. 52; see also *id.* at para. 110 (setting aside EU regulations mandating the disclosure to the general public of the recipients of EU agricultural subsidies to the extent that such mandatory disclosure related to natural persons).

³¹See *Tele2 Sverige AB*, Case C-203/15, *supra* note 3, para. 129.

³²Praesidium, *Note on the Draft Charter of Fundamental Rights of the European Union*, Charte 4473/00, (Oct. 11, 2000) http://www.europarl.europa.eu/charter/pdf/04473_en.pdf.

³³See *Tele2 Sverige AB*, Case C-203/15, *supra* note 3, para. 129.

³⁴See, e.g., CJEU, Joined Cases 46/87 & 227/88, *Hoechst v. Comm'n of the Eur. Communities* ECLI:EU:C:1989:337, Judgement of 21 Sept. 1989; CJEU, C-94/00, *Roquette Frères v. Directeur Général*, ECLI:EU:C:2002:603, Judgement of 22 Oct. 2002, at para. 29.

³⁵*Tele2 Sverige AB*, Case C-203/15, *supra* note 3, para. 127.

³⁶*Id.*

³⁷*Id.* at para. 128.

³⁸Charter of Fundamental Rights of the European Union, Dec. 7, 2000, 2000 O.J. (C 364) 1, at art. 8(1) [hereinafter CFREU].

³⁹CFREU art. 8(3).

case.⁴⁰ While the search of the recent landmark cases of the CJEU for elements of a substantial, meaningful, and consistent privacy concept proves surprisingly disappointing, the Court's statements relating to the essence of the right to privacy and the right to protection of personal data constitute a pleasant exception. In the *Digital Rights* decision, the CJEU stated that the interference by the generalized retention of, and the largely unlimited access by public authorities to, traffic and location data with the

right to privacy and the other rights laid down in Article 7 of the Charter. . . . are not such as to adversely affect the essence of those rights. Nor is that retention of data such as to adversely affect the essence of the fundamental right to the protection of personal data enshrined in Article 8 of the Charter. . . .⁴¹

According to the Court, the essence of the right to protection of personal data remained unaffected because the Data Retention Directive provided for certain data protection and security safeguards—implying that without such safeguards the essence of the right might have been affected—whereas the essence of the right to privacy remained unaffected because the Directive did not allow for the acknowledgment by the national authorities of the contents of the communication—implying that the possibility of such acknowledgment might have resulted in affecting the essence of the right.⁴² These remarks give additional evidence to the fact that the Court views—as indeed it should—the right to privacy and the right to protection of personal data as distinct in that each of them has a different essence.

But what about the “right to respect for private life with regard to the processing of personal data,”⁴³ as introduced in the *Schecke* case, and the implied notion of a combined, uniform right to respect for private life with regard to the processing of personal data? Assuming that the introduction of this notion in *Schecke* was not a mere *lapsus linguae*, here is one possible way of synthesis: In certain cases, the scope of the two fundamental rights in question may largely overlap. In the context of such cases, it may be rightly stated that the right to protection of personal data—Article 8 CFREU—is “closely connected with the right to respect of private life expressed in Article 7 of the Charter.”⁴⁴ Additionally, it is precisely such cases which may leave a limited remit for a combined “right to respect for private life with regard to the processing of personal data,”⁴⁵ as mentioned in the *Schecke* case. It remains disputable, though, whether the *Schecke* case itself would fall into such category of cases in which the two fundamental rights sufficiently overlap—see further below for another possible synthesis.⁴⁶ Still, and as a general rule, the right to privacy and the right to protection of personal data are not congruent or redundant but “distinct,” as correctly stated by the CJEU in the *Tele2* case.⁴⁷

II. Human Rights for Humans Only? On the Eligible Beneficiaries of the Right to Privacy

Up to the present day, the CJEU has not sufficiently clarified whether or to what extent the rights to privacy and protection of personal data are available to legal persons.⁴⁸

⁴⁰See *Digital Rights*, Joined Cases C-293/12 & C-594/12, *supra* note 5, paras. 39–40.

⁴¹*Id.* at paras. 39–40.

⁴²*Id.* at para. 39–40.

⁴³See *Schecke*, Joined Cases C-92/09 & C-93/09, *supra* note 30, para. 52.

⁴⁴*Id.* at para. 47.

⁴⁵*Id.* at para. 52.

⁴⁶See *Schecke*, Joined Cases C-92/09 & C-93/09, *supra* note 30 (describing the limited scope of the disclosure of personal data at stake in the *Schecke* case).

⁴⁷See *Tele2 Sverige AB*, Case C-203/15, *supra* note 3, para. 129.

⁴⁸See VALENTIN PFISTERER, UNTERNEHMENSPRIVATSPHÄRE 278 (2014) (discussing the concept of corporate privacy in EU constitutional law); Pfisterer, *supra* note 1, at 564–66.

In the *PNR* case, the CJEU, making reference to its decision in the *Schecke* case, noted with respect to the right to privacy that “that right concerns any information relating to an identified or identifiable individual.”⁴⁹ This statement appears to suggest that non-individuals—for example, companies, partnerships, associations, and other legal persons—cannot, as a matter of principle, benefit from the right to privacy.

In the *Schecke* decision, however, the CJEU held—somewhat less straightforward—that “the right to respect for private life with regard to the processing of personal data, recognised by Articles 7 and 8 of the Charter, concerns any information relating to an identified or identifiable individual. . . .”⁵⁰ Therefore, the CJEU continued:

[L]egal persons can claim the protection of Articles 7 and 8 of the Charter in relation to such identification [identification of company, by name, *vis-à-vis* the general public as recipient of public agricultural subsidies⁵¹] only in so far as the official title of the legal person identifies one or more natural persons.⁵²

This holding suggests that—at least in connection with the public disclosure of company-related data⁵³—a company can, indeed, rely on the right to privacy, or more precisely, the combined “right to respect for private life with regard to the processing of personal data”⁵⁴ introduced in that decision, provided that the company name identifies one or more natural persons—such as Dell or Daimler.⁵⁵

Finally—only a few years earlier—the CJEU held in the *Varec* case from 2008 that “the notion of ‘private life’ cannot be taken to mean that the professional or commercial activities of. . . legal persons are excluded. . . . Those activities can include participation [by a company] in a contract award procedure.”⁵⁶ Not mentioning any qualification nor, particularly, any reference to information relating to an individual, this statement appears to suggest that legal persons can, as a matter of principle, benefit from the protection of the right to privacy.

For purposes of consistency, the right to privacy should correctly be understood to be available to companies, whereas the right to protection of personal data is not. The reason for this is that, in the past, there has been a clearly distinguishable development whereby the CJEU jurisprudence relating to the right to privacy has consistently been expanding so as to include companies. In contrast, the right to protection of personal data has consistently been understood to be tied to the individual.

Between 1989 and 2002, the CJEU consciously expanded the scope of the right to respect for the home prong of the right to privacy to companies. In the *Hoechst* decision of 1989, the CJEU held that “[t]he protective scope of that article [Article 8 ECHR] is concerned with the development of man’s personal freedom and may not therefore be extended to business premises.”⁵⁷ About thirteen years later, in the *Roquette Frères* decision of 2002, the CJEU explained—diametrically opposed—that “the protection of the home provided for in Article 8 of the ECHR may in certain circumstances be extended to cover such [business] premises. . . .”⁵⁸ Only a few months before the

⁴⁹*PNR* Opinion 1/15, *supra* note 2, para. 122.

⁵⁰See *Schecke*, Joined Cases C-92/09 & C-93/09, *supra* note 30, para. 52.

⁵¹See *Schecke*, Joined Cases C-92/09 & C-93/09, *supra* note 30 (providing a brief description of the *Schecke* case).

⁵²See *id.* at 53.

⁵³See generally PFISTERER, *supra* note 48, at 278 (suggesting the pluralistic concept of corporate privacy).

⁵⁴See *Schecke*, Joined Cases C-92/09 & C-93/09, *supra* note 30, para. 52.

⁵⁵Gerrit Hornung, *EuGH: Keine Veröffentlichung von Empfängern von EU-Agrarsubventionen im Internet*, MULTIMEDIA UND RECHT 127 (2011) (presenting a critical approach as to this requirement) (“less convincing,” translation by author); Friederike Dratwa & Jana Werling, *Die erste Grundrechtsprüfung anhand der Charta der Grundrechte*, EUR. L. REP. 27 (2011).

⁵⁶See CJEU, C-450/06, *Varec v. Belgian State*, ECLI:EU:C:2008:91, Judgement of 14 Feb. 2008, at para. 48.

⁵⁷*Hoechst*, Joined Cases 46/87 & 227/88, *supra* note 34, para. 18.

⁵⁸*Roquette Frères*, Case C-94/00, *supra* note 34, para. 29.

Roquette Frères decision, the ECtHR handed down a judgment in which it expanded the personal scope of the right to the respect for home pursuant to Article 8 ECHR to legal persons in the *Société Colas Est* case from 2002.⁵⁹ In this decision, the ECtHR reiterated that “the Convention is a living instrument which must be interpreted in the light of present-day conditions. . . .”⁶⁰ This led the ECtHR to state:

Building on its dynamic interpretation of the Convention, the Court considers that the time has come to hold that in certain circumstances the rights guaranteed by Article 8 of the Convention may be construed as including the right to respect for a company’s registered office, branches or other business premises.⁶¹

Six years after the endorsement of the innovative step of the ECtHR by the CJEU in the *Roquette Frères* decision, the CJEU proceeded to assert in the *Varec* case that the expansion of the right to privacy to companies also applied to the respect for private life prong—see above.⁶² Only recently has the CJEU cast doubt on the consistency of this development by making the above-mentioned statements in the *Schecke* case⁶³ and the *PNR* case.⁶⁴

In contrast, the right to protection of personal data was developed based on, *inter alia*, the Data Protection Directive and in the opinion of the Convention, “is to be exercised under the conditions laid down in the above [Data Protection] Directive. . . .”⁶⁵ Pursuant to the Data Protection Directive, however, the term personal data was defined as any information relating to an identified or identifiable natural person.⁶⁶ This understanding was confirmed in connection with the enactment of the General Data Protection Regulation.⁶⁷ It is, therefore, of consequence to reserve the right to protection of personal data to individuals. Against this background, the statement made by the CJEU in the *PNR* case⁶⁸ appears inaccurate insofar as it relates to the right to privacy whereas it would correctly describe the precondition, as discussed above, of the right to protection of personal data.

The question again, is how to tie in the “right to respect for private life with regard to the processing of personal data,”⁶⁹ as mentioned in the *Schecke* case. Here is another possible way of synthesis: As companies cannot rely on the right to protection of personal data and are left, instead, to rely on the right to privacy, they may challenge incidents of data breaches or disclosure of company-related data—as in the *Schecke* case⁷⁰—only based on that right to privacy. The interpretation of the right to privacy in this context may be informed by the right to protection of personal data, resulting in a limited companies’ right to respect for private life with regard to the processing of personal data. To ensure that there is sufficient reconnection to the individual, as required by the right to protection of personal data, the reliance by a company on this “companies’

r-

⁵⁹*Société Colas Est. v. France*, App. No. 37971/97, Eur. Ct. H.R. (2002).

⁶⁰*Id.* at 41.

⁶¹*Id.* at 41.

⁶²See *Varec*, Case C-450/06, *supra* note 56, para. 48; see also PFISTERER, *supra* note 48 (providing a judicial discourse leading to the acknowledgment by the CJEU of the corporate right to privacy); see also Pfisterer, *supra* note 1 (same).

⁶³See *Schecke*, Joined Cases C-92/09 & C-93/09, *supra* note 30, paras. 52–53.

⁶⁴See *PNR* Opinion 1/15, *supra* note 2, para. 122.

⁶⁵*Praesidium*, *supra* note 32, at 11.

⁶⁶Data Protection Directive *supra* note 15, art. 2(a).

⁶⁷See General Data Protection Regulation 2016/679, O.J. (L 119) 1, at art. 4(1).

⁶⁸*PNR* Opinion 1/15, *supra* note 2, para. 122 (“[T]hat right [the right to privacy] concerns any information relating to an identified or identifiable individual.”).

⁶⁹*Schecke*, Joined Cases C-92/09 & C-93/09, *supra* note 30, para. 52.

⁷⁰See *Schecke*, Joined Cases C-92/09 & C-93/09, *supra* note 30 (describing the limited scope of the disclosure of personal data at stake in the *Schecke* case).

ight” is contingent upon its official name identifying one or more natural persons, as required by the CJEU in the *Schecke* case.⁷¹

III. Important, but Why? On the Particular Importance of the Right to Privacy

The CJEU has repeatedly stressed the important role of the right to privacy, though, without giving any reasons therefore. In the *Schrems* and *Tele2* cases, the CJEU highlighted the “importance of both the fundamental right to respect for private life, guaranteed by Article 7 of the Charter, and the fundamental right to the protection of personal data, guaranteed by Article 8 thereof. . . .”⁷² In both instances, the Court made reference to the emphasis given to such importance in settled case-law, citing, in each case, a number of previous decisions. Neither in the *Schrems* and *Tele2* cases, nor in the cited case law, however, does the Court specifically elaborate on the importance of these rights—giving reasons, providing examples, or relating the rights to other rights perceived as less important. Rather, in the *Tele2* case, the Court goes on stating that “[t]he same is true of the right to freedom of expression in the light of the particular importance accorded to that freedom in any democratic society,” and explains that this right “constitutes one of the essential foundations of a pluralist, democratic society, and is one of the values on which, under Article 2 TEU, the Union is founded.”⁷³ Why does the Court elaborate on the importance of the right to freedom of expression but not on that of the rights to privacy or protection of personal data? The reason might be that the Court—despite its initial steps towards figuring out the essence of these rights—has not yet sufficiently thought through their ultimate object and purpose and, thus, particular importance.⁷⁴

IV. What For? On the Right to Privacy’s Function in Society

The CJEU held in the *PNR* case that “the rights enshrined in Articles 7 and 8 of the Charter are not absolute rights, but must be considered in relation to their function in society.”⁷⁵ The statement that the rights to privacy and protection of personal data are not absolute is a truism. The mere existence of Article 52 CFREU, which uniformly sets forth the requirements for interferences with any of the guarantees contained in the CFREU, implies that such guarantees, including those in Articles 7 and 8 CFREU, are open to justified government interference. Furthermore, Article 8(2) CFREU sets forth specific requirements for data processing—for example, interference with the right to protection of personal data—in compliance with the CFREU, thus also implying that the right guaranteed in Article 8(1) CFREU is open to justified government interference. More importantly, however, with regard to the statement of the CJEU relating to the function in society of the rights to privacy and protection of personal data: Neither in this opinion, nor in the case law cited—or in the case law cited in such case law—does the CJEU explain or further elaborate on the function in society of these rights. In view of the missing discussion of the specific importance of the rights to privacy and protection of personal data—see above—this is somewhat unsurprising and seems to be similarly related to the persisting uncertainty as to the ultimate object and purpose of these rights.

⁷¹See *Schecke*, Joined Cases C-92/09 & C-93/09, *supra* note 30, para. 53.

⁷²*Schrems*, Case C-362/14, *supra* note 4, para. 39; see also *Tele2 Sverige AB*, Case C-203/15, *supra* note 3, para. 93.

⁷³See *Tele2 Sverige AB*, Case C-203/15, *supra* note 3, para. 93.

⁷⁴See *Marckx v. Belgium*, App. No. 6833/74, Eur. Ct. H.R., at para. 31 (1979) (“[T]he object of [Article 8(1) ECHR] is ‘essentially’ that of protecting the individual against arbitrary interference by the public authorities.”). While not directly applicable, this might serve as a starting point for the CJEU.

⁷⁵*PNR* Opinion 1/15, *supra* note 2, para. 136.

V. The Essence of the Right to Privacy—Getting to the Heart of It

Finally, and as mentioned above, the statements of the CJEU relating to the essence of the right to privacy seem to be the only meaningful contribution to the conceptualization of the right to privacy originating from the recent landmark cases. The Court in the *Digital Rights* case and the *Tele2* case found that the essence of the right to privacy remained unaffected, because the Data Retention Directive and the Swedish legislation passed on the basis of the Article 15(1) exemption of the Directive on Privacy and Electronic Communications, respectively, did not allow for the acknowledgment by the respective national authorities of the contents of the communication.⁷⁶ The CJEU, conversely, did find an interference with the essence of the right to privacy in the *Schrems* case.⁷⁷ In this decision, the CJEU held that “legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter.”⁷⁸ Never before had the CJEU or the ECtHR considered an interference with the right to privacy as comprising the essence of this fundamental right.⁷⁹ The decision of the CJEU in the *Schrems* case has therefore been characterized as a “pathbreaking development” or a “major contribution to the understanding of the structure and legal effect of fundamental rights under the Charter.”⁸⁰ Unfortunately, the decision does not reveal why exactly—for example, for what reasons and due to what interests—the CJEU considers the acknowledgment by the national authorities of the contents of communication between individuals to constitute an interference with the essence of privacy. Also, the Court unfortunately does not, in the same context, discuss whether or not the measure also constituted an interference with the essence of the right to protection of personal data.⁸¹

While it is a positive step that the CJEU revealed what it considers the essence of the right to privacy, the Court should elaborate more deeply on this point in the future. Also, going forward, the Court may wish to add statements clarifying the particular importance, the function in society, as well as the ultimate object and purpose of the right to privacy to any future statement relating to the essence of this right.

D. Distinguish, Explain, Clarify, Elaborate, and Move Beyond—in Sum: Conceptualize! How to Adjudicate Privacy in the Future

In recent years, the CJEU has impressively brought to bear the protection of the fundamental rights to privacy and protection of personal data as contained in the CFREU. The Court’s decisions in the *Digital Rights*, *Schrems*, *Tele2*, and *PNR* cases have reshaped the political and legal landscape in Europe and beyond. By restricting the powers of the governments of EU Member States and annulling legislative acts enacted by the EU legislator, the decisions had, and continue to have, effects well beyond the respective individual cases.

Despite their strong impact on privacy and data protection across Europe, these landmark decisions reveal a number of flaws and inconsistencies in the conceptualization of the rights to privacy and protection of personal data as endorsed and interpreted by the CJEU. These shortcomings relate to the relationship between the right to privacy and the right to protection of personal data, the eligible beneficiaries of the right to privacy as well as the particular importance, the function in society, and the essence of the right to privacy. Overall, the failure

⁷⁶*Digital Rights*, Joined Cases C-293/12 & C-594/12, *supra* note 5, para. 39; *Tele2 Sverige AB*, Case C-203/15, *supra* note 3, para. 100–01; see also *PNR* Opinion 1/15, *supra* note 2, para. 151.

⁷⁷*Schrems*, Case C362/14, *supra* note 4, para. 94.

⁷⁸*Id.*

⁷⁹See Martin Scheinin, *The Essence of Privacy, and Varying Degrees of Intrusion*, VERFASSUNGSBLOG (Oct. 7, 2015) <http://verfassungsblog.de/the-essence-of-privacy-and-varying-degrees-of-intrusion-2>.

⁸⁰*Id.*

⁸¹See *Kuner*, *supra* note 24, at 892.

by the CJEU to come up with, maintain, and develop a consistent concept of the fundamental rights to privacy and protection of personal data results in a lower degree of certainty, reliability, and predictability with a view to its current and future jurisprudence.

With regard to the relationship between the right to privacy and the right to protection of personal data—for purposes of consistency—the Court should confirm and clarify, where appropriate, that these guarantees should be understood to be fundamental rights distinct from each other with different objects, purposes, and essences. With a view to the eligible beneficiaries of the right to privacy, the Court should make an effort to clarify whether, to what extent or under what conditions legal persons are entitled to benefit from the protection of this right, and potentially, the right to protection of personal data. Furthermore, in relation to the particular importance of the right to privacy, the CJEU should reflect upon and come up with a comprehensive and thought-out explanation as to why the rights to privacy and protection of personal data are of such particular importance and to what effect. Also, with regard to the function of the rights to privacy and protection of personal data in society, the Court should not confine itself to citing previous case law—which, besides, does not address this issue—but rather provide an explanation and elaborate on the specific function of these rights in our society. Finally, regarding the essence of the right to privacy—and the right to protection of personal data—the Court should move beyond what was stated and implied in the *Digital Rights* and *Schrems* cases and provide a more in-depth rationale as to why the measures in dispute compromise the respective essence of the right to privacy and right to protection of personal data. In consideration of the missing pieces regarding the distinctiveness of the right to privacy and to protection of personal data, the eligible beneficiaries, as well as the particular importance, function in society, and essence of the right to privacy—and the right to protection of personal data—the CJEU should develop an integrated, comprehensive, and consistent concept of the right to privacy and the right to protection of personal data. In doing so, the Court would significantly increase the degree of certainty, reliability, and predictability with a view to its future jurisprudence and ultimately strengthen the rule of law in Europe.