German Law Journal (2021), **22**, pp. 31–44
doi:10.1017/glj.2020.101

CAMBRIDGE UNIVERSITY PRESS

ARTICLE

The Democratic Impact of Strengthening European Fundamental Rights in the Digital Age: The Example of Privacy Protection

Sandra Seubert* and Carlos Becker**

Department of Political Science, Goethe University, Frankfurt, Germany

(Received 21 April 2020; revised 04 June 2020; accepted 05 June 2020)

Abstract

In times of digital pervasion of everyday life, the EU has strengthened a normative idea of European fundamental rights, especially by referring to a strong notion of privacy protection. A normative corridor is evolving with the "right to privacy" at its heart, a right that will be instrumental in shaping the European legal architecture's future structure. In this Article we argue that the constitutional protection of privacy rights is not only of individual relevance but also of major democratic significance: it protects the integrity of the communication structures that underpin democratic self-determination. The debate on privacy protection, however, often lacks a democratic understanding of privacy and misses its public value. Following an interactionist understanding of privacy and a discourse-theoretical model of democracy, our argument puts forward a conceptual link between privacy and the idea of communicative freedom. From this perspective, the substantiation of a European fundamental right to privacy can be seen as a possible contribution to promoting European democracy in general.

Keywords: privacy; European fundamental rights; communicative freedom; digitalization; European democracy

"Our freedom is built on what others do not know of our existences."
Alexander I. Solzhenitsyn

A. Introduction

The digitalization of everyday life is pervading modern societies. This development is accompanied by vigorous academic debates, which are seeking to reassess the normative foundations of democracy together with its relationship to digitalization.[1] More particularly, these discussions firmly place

*Sandra Seubert received her Ph.D in Political Science from Free University Berlin. She is a professor of Political Theory at Goethe-University, Frankfurt a.M.

**Carlos Becker received his Ph.D in Political Science from Goethe University. He was a Research Associate at Goethe University, Frankfurt a.M. until Summer 2020. He currently works as project coordinator for the scientific monitoring of federal programs of democracy promotion.

[1]For an overview, see Ralf Lindner & Georg Aichholzer, *E-Democracy: Conceptual Foundations and Recent Trends*, *in* EUR. E-DEMOCRACY IN PRAC. 11 (2020). For further discussions, see KATRIN VOSS, INTERNET UND PARTIZIPATION: BOTTOM-UP ODER TOP-DOWN? (POLITISCHE BETEILIGUNGSMÖGLICHKEITEN IM INTERNET) (2014); Robin Celikates, *Digital Publics, Digital Contestation—A New Structural Transformation of the Public Sphere?*, *in* TRANSFORMATIONS OF DEMOCRACY: CRISIS, PROTEST, LEGITIMATION 159 (Robin Celikates et al. eds., 2015); Jürgen Habermas, *Moralischer Universalismus in Zeiten politischer Regression*, 48 LEVIATHAN 7 (2020); Jürgen Habermas, *Political Communication in Media Society: Does Democracy Still Have an Epistemic Dimension? The Impact of Normative Theory on Empirical Research*, 16 COMM. THEORY 411 (2006);

their focus on the value of privacy and its protection.[2] However, given the global character of digitalization, together with its transnational technical infrastructure and ownership make-up, the relationship between digitalization, democracy, and privacy can no longer be conceived as being confined to nation-states. Against this backdrop, the European Union as a political and legal actor has become increasingly important, which in turn has sparked its own academic debate and further scrutiny.[3]

With the introduction of the EU Charter of Fundamental Rights, a mandatory catalogue of rights has come into force, aimed at providing a constitutional underpinning of European Union law.[4] Interestingly enough, normative substantiation of European fundamental rights can be seen as being advanced especially in the field of digital and internet policy—a process largely driven and strengthened by Europe's legal institutions, primarily the Court of Justice of the European Union (CJEU). Through its attempts to impose normative constraints on digital transformation by way of landmark decisions—*Schrems I, the right to be forgotten*—European case law has moved to the focus of public attention. Here, the Court has been using the multidimensional *right to privacy*[5] for the purpose of exemplifying and advancing the strengthening and assertiveness of European fundamental rights. Between the regulatory purpose of European law centered on the European Single Market and a commitment to fundamental rights, a "normative corridor" is evolving with the right to privacy at its very heart, a right that will be instrumental in shaping the European legal architecture's future structure.[6] This increasing importance of privacy protection in Europe is not only to be understood in relation to the protection of individuals' rights, however, but also with regard to its relevance for democratic societies; by strengthening people's personal freedom, European privacy protection is, at the same time, proving to be essential for the development and flourishing of democratic practices conceptualized as collective acts of free communication.

The specifically democratic significance of the constitutional protection for individual privacy rights in Europe will form the focus of our contribution here. Importantly, though, we will place this debate in the context of the prevailing political challenges posed by digital transformation. It

Taewoo Nam, *A Tool for Liberty or Oppression? A Cross-National Study of the Internet's Influence on Democracy*, 34 Telematics & Informatics 538 (2017); Nathaniel Persily, *Can Democracy Survive the Internet?* 28 J. Democracy 63 (2017).

[2]*See* Engin Isin & Evelyn Ruppert, Being Digital Citizens (2015); Paul Schwartz, *Privacy and Democracy in Cyberspace*, 52 Vand. L. Rev. 1607 (1999); Sandra Seubert & Peter Niesen, Die Grenzen des Privaten (2010); Zizi A. Papacharissi, A Private Sphere. Democracy in a Digital Age (2010).

[3]*See* Marie-Pierre Granger & Kristina Irion, *The Right to Protection of Personal Data: The New Posterchild of European Union Citizenship?*, *in* Civil Rights and EU Citizenship 279 (Sybe De Vries et al. eds., 2018); Kristina Irion, *A Special Regard: The Court of Justice and the Fundamental Rights to Privacy and Data Protection*, *in* Gesellschaftliche Bewegungen. Recht unter Beobachtung und in Aktion 873 (Ulrich Faber et al. eds., 2016); Bilyana Petkova, *Privacy as Europe's First Amendment* 25 Eur. L.J. 140 (2019).

[4]For a discussion of the role of fundamental rights in EU law, see the special issue on the "essence" of fundamental rights in 20 German L.J. 763, 763–939 (2019). *See generally* Jürgen Kühling, *Fundamental Rights*, *in* Principles of European Constitutional Law (Armin von Bogdandy & Jürgen Bast eds., 2011).

[5]It is worth mentioning that neither European Union law nor German law features a single piece of legislation actually referencing the *right* to privacy. For a comprehensive account of this, see Johannes Eichenhofer, *Rechtswissenschaftliche Perspektiven auf Privatheit*, *in* Privatsphäre 4.0 155 (Hauke Behrendt et al. eds., 2019). The protection of *private* life is, at least conceptually, enshrined in European law. In the following discussion, therefore, the right to privacy is taken to comprise all rights, which, in the broadest sense, pertain to protection of the private sphere, personal communication, and personal data; in other words, data protection. Whilst respect for private life, interaction relationships, and data protection will not be used synonymously, they will be seen as complementary such that for the purpose of this article, they can be subsumed under the right to privacy. For a well-argued, albeit legally not uncontroversial, summary of this subject matter, see Christoph Gusy, *Datenschutz als Privatheitsschutz oder Datenschutz als Privatheitsschutz?* 45 Europäische Grundrechte Zeitschrift 244 (2018).

[6]*See* Sybe de Vries, *The EU Single Market as 'Normative Corridor' for the Protection of Fundamental Rights: The Example of Data Protection*, *in* The EU Charter of Fundamental Rights as a Binding Instrument: Five Years Old and Growing 235, 236 (Sybe de Vries et al. eds., 2015).

https://doi.org/10.1017/glj.2020.101 Published online by Cambridge University Press

is, after all, the rapidly transforming structure of digital communication and data processing that is leading to new types of threats to communicative freedom. Therefore, whilst we will be primarily concerned with constitutional questions and the democratic interpretation of privacy protection, it is the digitalization of everyday communication and its potential implications that drives home the enormous significance of these questions.

This Article proceeds in three steps. First, we examine how the right to privacy within Europe's multidimensional legal architecture assumes importance as a fundamental right, considering its substantive underpinning in the form of legislation enforced by individual rulings. We then go on to explore the consequences of the substantiation of European fundamental rights for democratic politics, based on the example of privacy protection. Second, we look at how the relationship between privacy and democracy is to be understood from a normative perspective. Following a cursory critique of individual rights-based privacy theories, we put forward a social understanding of privacy, which, in essence, is geared towards an interactionist conception of social freedom. Our argument then expands on the conceptual link between privacy and the idea of communicative freedom. This will prove to be particularly useful when it comes to explicating the democratic value of privacy and its significance for a digital communication structure. Third, and finally, we combine these first two components and provide an overview covering the democratic effects of European privacy protection.

B. A Fundamental Right to Privacy in Europe?

Ironically, the need to improve privacy protection in Europe has ultimately arisen from new threats that have come to light in the wake of digital transformation. The supranational data economy and the mass surveillance of everyday digital communication, particularly by the Five Eyes Alliance,[7] have been decisive drivers behind the initiative led by European legal institutions and the European Parliament to ensure better and more effective protection of the fundamental right to privacy.

On the one hand, this initiative sought to rein in the unfettered data and information market, where the absence of standards for data protection has been associated with economic advantages, giving rise to tensions between EU countries with differing levels of protection. On the other hand, the Snowden surveillance disclosures in particular have highlighted the need for the dedicated protection of personal data and privacy not only in the EU, but also with regard to non-member states and their potential intelligence activities.

Within the EU's multi-level governance system, the fundamental rights dimension of respect for private life and the protection of personal data has certainly prevailed for some time now. As long ago as 1950, Article 8 of the European Convention on Human Rights (ECHR) stipulated the right to private and family life. This right can be collectively challenged only if a high threshold of very important public interest is reached, with Article 8 placing particular emphasis on the protection of private "correspondence."[8] As a treaty under international law, Article 8 not only serves as a normative source of European privacy protection standards,[9] but, through its incorporation within the Convention's catalogue of fundamental rights, also establishes the central importance of privacy within the EU's constitutional framework. Privacy's status as a fundamental right has also been reinforced not just through additional EU treaties and statute books, but has also

[7]Generally, "5-Eyes" refers to the cooperation between the intelligence services of the United States, Canada, the United Kingdom, Australia, and New Zealand, which attracted much public attention, particularly after Edward Snowden's disclosures of surveillance practices. *See* Glenn Greenwald, Die globale Überwachung: Der Fall Snowden, die amerikanischen Geheimdienste und die Folgen 175–92 (2014).

[8]European Convention for the Protection of Human Rights, art. 8(1) (1950).

[9]*See* Granger & Irion, *supra* note 3, at 3–4.

https://doi.org/10.1017/glj.2020.101 Published online by Cambridge University Press

received further supplementation through the addition of the fundamental right to data protection.

Both Article 39 of the Treaty of Lisbon and Article 16 of the Treaty on the Functioning of the European Union confer on data protection a status equivalent to that of a fundamental right. This obliges all EU bodies and institutions to handle sensitive data properly and in a manner that is appropriate in relation to the specified purpose of its use, whilst also extending this right to all EU citizens as individuals. Articles 50 and 51 of the draft European Constitution, albeit subsequently rejected, likewise attached the importance of fundamental rights to the protection of privacy and personal data.[10]

This emphasis on privacy applies in particular to the EU Charter of Fundamental Rights (CFR), which, in Articles 7 and 8, assigns central importance to respect for private life as well as to the protection of personal data and its usage. In sum, the protection of privacy is enshrined in international law through the ECHR, institutional and procedural law through the TEU/TFEU, as well as the EU Charter of Fundamental Rights (CFR), and is thus reinforced as a pillar of European legal architecture.[11]

That said, the Charter of Fundamental Rights has proven to be especially important in this context, because, as a legal framework, the CFR is functionally equivalent to a constitution. This makes the CJEU something akin to a "Court of Fundamental Rights" (*Grundrechtsgericht*),[12] whose substantive rulings also shape the structure and scope of European fundamental rights.[13] This pertains to both the internal European hierarchy of fundamental rights, vis-à-vis the EU's fundamental freedoms[14], and the precedence of European Union law over member states' national laws. Taking the right to privacy as an example, the question of how the substantiation of fundamental rights in Europe might affect democracy is particularly pertinent with regard to the CFR and CJEU rulings. However, since the CJEU's inception, its interpretation of European fundamental rights has been the subject of criticism and has been viewed with ambivalence, particularly in Germany.[15] This has rested on a suspicion that the CJEU would, in case of doubt, always prioritize

[10]For an overview, see Ulf Brühann, *EUV Art. 39—Datenschutz*, *in* EUROPÄISCHES UNIONSRECHT 436 (Hans von der Groeben et al. eds., 2015); Ulf Brühann, *AEUV Art. 16—Datenschutz*, *in* EUROPÄISCHES UNIONSRECHT 982 (Hans von der Groeben et al. eds., 2015).

[11]Bilyana Petkova even goes as far as to refer to privacy as "Europe's First Amendment." *See* Petkova, *supra* note 3, at 140–42, 153–54. Rather controversially, Petkova thus interprets privacy in Europe as mirroring the status of the right to freedom of expression in the U.S., suggesting it should be seen not only as being at the heart of the entire legal architecture, but also as having an integrating function comparable to that of the freedom of expression at the time of the American civil rights movement. *See id.* at 144–46, 148–54.

[12]Jürgen Kühling, *Der Fall der Vorratsdatenspeicherungsrichtlinie und der Aufstieg des EuGH zum Grundrechtsgericht*, 33 NEUE ZEITSCHRIFT FÜR VERWALTUNGSRECHT 681, 684 (2014).

[13]*See* ULRICH HALTERN, EUROPARECHT: DOGMATIK IM KONTEXT 579–85 (3d ed. 2017).

[14]*See* Case C-36/02, Omega, 2004 E.C.R. I-09609.

[15]This refers to both the relationship between fundamental freedoms and fundamental rights in the European Single Market, as well as the specific quality and limitations of CJEU case law. On the one hand, the CJEU stood accused of prioritizing, in case of doubt, the fundamental freedoms of the internal market primacy over fundamental rights. On the other hand, it was highlighted that the protection of fundamental rights by European legal institutions was either too strong or too weak. *See* Johannes Masing, *Einheit und Vielfalt des Europäischen Grundrechtsschutzes*, 70 JURISTEN ZEITUNG 477, 486–87 (2015). In particular, the German Federal Constitutional Court and the corresponding commentary have repeatedly expressed their concerns about the alleged threat posed by a dilution of fundamental rights standards. *See* HALTERN, *supra* note 13, at 446–48. Criticism has been articulated from both an *institutional* perspective, regarding the unauthorized extension of CJEU competences to encompass areas that are not defined in European Union law, and from a *substantive* perspective, targeting its specific interpretation of fundamental rights. This debate culminated in relation to the *Åkerberg Fransson* and *Melloni* rulings. In this context, the CJEU not only sought a considerable extension of its competences, but also threatened to dilute standards of fundamental rights protection on the grounds of harmonization of European legal systems. *See* HALTERN, *supra* note 13, at 698–701. *See also* Asteris Pliakos & Georgios Anagnostaras, *Fundamental Rights and the New Battle over Legal and Judicial Supremacy: Lessons from Melloni*, 34 Y.B. EUR. L. 97, 104–06 (2015). The recent rulings by the German Federal Constitutional Court on the *Right to be Forgotten* will again reframe the relation of national and European law, because the German Court allows itself, with that ruling, a direct reference to the CFR and its fundamental rights and, with that, opens up a "parallel

https://doi.org/10.1017/glj.2020.101 Published online by Cambridge University Press

the fundamental freedoms of the Single Market over fundamental rights. Furthermore, given the harmonization of European legal architectures, it was feared that this would lead to a general decline in the standards of fundamental rights protection.

These fears were made explicit in the context of European legal rulings on privacy and data protection issues. It was expected that the economic importance of digital industries and the relevance of security policy issues could, in case of doubt, be used to form an argument against strengthening privacy as a fundamental right. Given this backdrop, all the more surprising, therefore, has been the CJEU robust advocacy for a strengthening of privacy protection as a fundamental right based on Articles 7 and 8 of the CFR. The CJEU is thus positioning itself as a strong European court of fundamental rights vis-à-vis the EU and its member states.[16] Ultimately, there are three key rulings supporting this impression: *Digital Rights Ireland*,[17] *Google Spain*,[18] and *Schrems I*.[19]

The *Digital Rights Ireland* ruling of 2014 concerned the EU Data Retention Directive, which afforded authorities wide-ranging access to electronic communications data for no specific purpose. The CJEU considered this directive to be a serious infringement of the fundamental rights enshrined in Articles 7 and 8 of the CFR.[20] It was seen as constituting an "encroachment on the fundamental rights of virtually the entire European population,"[21] leading to the unavoidable conclusion "that by adopting Directive 2006/24, the European Union legislature had exceeded the limits imposed by compliance with the principle of proportionality in the light of Articles 7, 8 and 52(1) of the Charter."[22] For the first time, the CJEU subsequently declared as null and void an *entire* EU directive that had previously been agreed upon by the member states[23] and, in so doing, rigorously employed the CFR as the basis for a judicial review procedure.[24]

In its *Google Spain* ruling, shortly after the Directive 2006/24 case, the CJEU resumed this strict adherence to protecting privacy as a fundamental right. This ruling concerned possible infringements of personal integrity resulting from online search engine hit lists. On the basis of Articles 7 and 8 of the CFR, the CJEU derived the "right to be forgotten," which can oblige internet search engine operators to remove certain links from their lists of search results. As a result, this ruling gives the right to privacy precedence over both public interests and associated rights as well as over the commercial interests of the internet search engine operators.[25]

applicability" of European fundamental rights and, therefore, a new form of "heterarchy between European and domestic constitutional law." For more on this debate, see Matthias Goldmann, *As Darkness Deepens: The Right to be Forgotten in the Context of Authoritarian Constitutionalism*, 21.5 GERMAN L.J. 45 (2020). On potential political and judicial effects, see Matej Avbelj, *The Federal Constitutional Court Rules for a Bright Future of Constitutional Pluralism*, 21.5 GERMAN L.J. 27 (2020); Dana Buchardt, *Backlash Against the Court of Justice of the EU? Recent Jurisprudence of the German Constitutional Court on EU Fundamental Rights as a Standard of Review*, 21.5 GERMAN L.J. 1 (2020).

[16]De Vries, *supra* note 6, at 244–46; Irion, *supra* note 3, at 879–82, 886–87; Petkova, *supra* note 3, at 148–52.

[17]EJC, Joined Cases 293 & 594/12, Digital Rights Ireland, ECLI:EU:C:2014:238, Judgement of 8 April 2014, http://curia.europa.eu/juris/liste.jsf?num=C-293/12&language=EN [hereinafter Digital Rights Ireland].

[18]CJEU, Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos, ECLI:EU:C:2014:317 (May 13, 2014), http://curia.europa.eu/juris/liste.jsf?num=C-131/12 [hereinafter Google Spain].

[19]CJEU, Case C-362/14, Schrems v. Data Protection Commissioner, ECLI:EU:C:2015:650 (Oct. 6, 2015), http://curia.europa.eu/juris/liste.jsf?num=C-362/14 [hereinafter Schrems I].

[20]*Digital Rights Ireland* at paras. 52–63.

[21]*Id.* at para. 56.

[22]*Id.* at para. 69.

[23]The CJEU had already created a precedent in the area of privacy protection with the *Schecke Eifert* ruling. In this case, the CJEU for the first time overruled European law by referring to Articles 7 and 8 of the Charter of Fundamental Rights. *See* Petkova, *supra* note 3, at 148.

[24]*See* HALTERN, *supra* note 13, at para. 1368; Irion, *supra* note 3, at 882–84.

[25]The right to be forgotten is weakened where there is justified public interest in specific information. This is mainly the case if the person in question occupies a public position or any form of office. *See Google Spain* at paras. 97–98. For a general discussion, see Bilyana Petkova, *Data Privacy Rights and Citizenship: Notes on Federalism All the Way Up*, *in* EU CITIZENSHIP AND FEDERALISM. THE ROLE OF RIGHTS 540, 542–43 (Dimitry Kochenov ed., 2017); Volker Boehme-Neßler,

https://doi.org/10.1017/glj.2020.101 Published online by Cambridge University Press

The CJEU took an even stronger position with the *Schrems I* ruling, which concerned what was known as the "Safe Harbour" data protection agreement between the U.S. and the EU (International Safe Harbour Privacy Principles). Once again, explicitly referring to Articles 7 and 8 of the CFR, the CJEU declared the transatlantic data protection agreement as null and void on the grounds that the U.S. did not guarantee appropriate levels of protection for the fundamental right to privacy and that, as a result of mass surveillance, personal data was being stored indiscriminately. This meant that "a regulation allowing the authorities full access to the content of electronic communication violated the essence of the fundamental right to a private life guaranteed by Article 7 of the Charter."[26] Besides further strengthening and shaping the European fundamental right to privacy, which prohibits mass storage of private acts of communication and access to those communications that are not linked to specific purposes, the CFR, with the CJEU's help, also began influencing the level of data protection in third countries where "the laws and the practice of these countries [is unable to guarantee] an adequate level of protection."[27]

A crucial point here, however, is that the CJEU, again for the first time, overruled European secondary law by referring to a breach in the essence of fundamental rights.[28] This not only points to a serious violation of a fundamental right, but also means that this violation cannot be legitimized or offset on the grounds of other interests and rights.[29] The overall picture that emerges is one where privacy protection not only plays a central role[30] within the European legal architecture, but is also used to advance the substantiation of European fundamental rights more generally.[31]

This Article seeks to identify this substantiation of the right to privacy as a fundamental right in Europe and provide an outline of its potential democratic implications. Here, our starting point will have less to do with the overall democratic importance of fundamental rights for democratic systems. Instead, our focus will be directed towards the democratic value of privacy. From this perspective, the specific democratic importance of the constitutional protection of privacy rights

Das Recht auf Vergessenwerden: Ein neues Internet-Grundrecht im Europäischen Recht, 33 NEUE ZEITSCHRIFT FÜR VERWALTUNGSRECHT 825, 829–31 (2014). On the right to be forgotten in the GDPR see Michael Kubis, *Das Recht auf Vergessenwerden*, 41 DATENSCHUTZ UND DATENSICHERHEIT 583 (2017).

[26]*Schrems I* at para. 94.

[27]*Id.* at para. 107. *See also id.* at paras. 45–47, 72–74. In part, extending the scope of European privacy rights is also reflected in the GDPR, where all users of digital communication technologies are explicitly classified as potential subjects to be protected—in other words, not just European Union citizens. Although this is, of course, a rather different situation, even here it is evident how tensions can develop between national and regional legal systems as well as the global communication flows on the internet. As a key actor within the world of global communication, however, the European initiative for the protection of privacy could develop substantial power by obliging third parties to guarantee a similar level of protection.

[28]For a general discussion of the increasing prominence of the concept of "essence" in the discourse of fundamental rights in EU law, see Mark Dawson, Orla Lynskey, Elise Muir, *What is the Added Value of the Concept of the "Essence" of EU Fundamental Rights?*, 20 GERMAN L.J. 763 (2019). With regard to CJEU rulings on privacy and the role of *Schrems* in particular, see Maja Brkan, *The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning*, 20 GERMAN L.J. 864 (2019); Koen Lenaerts, *Limits on Limitations: The Essence of Fundamental Rights in the EU*, 20 GERMAN L.J. 779 (2019).

[29]*See* Petkova, *supra* note 3, at 150. Subsequently, the *Privacy Shield* framework was developed as a new data protection agreement, the effectiveness of which has once again been called into question by several parties. This, in turn, has been a key contributory factor in the development of what has been dubbed the *Schrems II* procedure, which is currently being debated by the CJEU after the case was once again referred to the CJEU by the Supreme Court of Ireland in a preliminary ruling procedure. Given that the CJEU has become known for its rigorous administration of justice in relation to data protection and privacy, there has been significant opposition to the adoption of this procedure by the CJEU, particularly from Facebook. For example, see Mary Carolan, *Facebook Loses Supreme Court Appeal in Max Schrems Case*, IRISH TIMES (May 31, 2019), https://www.irishtimes.com/business/technology/facebook-loses-supreme-court-appeal-in-max-schrems-case-1.3910710; Natasha Lomas, *Facebook Fails to Stop Europe's Top Court Weighing in on the EU-US Data Transfers*, TECHCRUNCH (Jun. 4, 2019), https://techcrunch.com/2019/06/04/facebook-fails-to-stop-europes-top-court-weighing-in-on-eu-us-data-transfers.

[30]This position is substantiated by the fact that the CJEU has convened as a Grand Chamber for issues concerning privacy and data protection. As this is something it had previously done only in a small number of prominent cases, this is further evidence of the pivotal importance of these issues for the CJEU. *See* Irion, *supra* note 3, at 876–78.

[31]Granger & Irion, *supra* note 3, at 283–85, 295–302.

https://doi.org/10.1017/glj.2020.101 Published online by Cambridge University Press

is revealed by approaching the value of privacy within the context of democratic theory, conceiving of the right to privacy as comprising more than merely individual rights.

C. The Democratic Value of Privacy

For some time now, academic debate on privacy has been noticeably shifting away from a traditional liberal paradigm of privacy rights. In the liberal tradition, privacy and personal autonomy are fundamentally linked through a particular modern understanding of individual freedom. This understanding is negative in the sense of focusing on independence—from traditional roles, authorities, and conventions—and includes the right "to shut the world out" from certain personal decisions concerning the "good life."[32] It is pre-political to the extent that it focuses on rights that persons can "naturally" claim prior to any normative justification to a democratic public. Closely relating privacy with notions of individual retreat, this understanding was transferred into law at a very early stage with the notion of privacy as the "right to be left alone,"[33] which went on to shape views regarding case law on privacy for decades, particularly in the U.S. Similar to the current renaissance of privacy research, Warren and Brandeis' defense of privacy was also a response to technological developments of their time, particularly photography and its first commercial usage, which constituted a new threat to private life.[34] They thus developed an interpretation of privacy that was based primarily on ownership—image rights, for instance—and which, at the same time, was linked to a strong notion of individual access and control.[35]

> The common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be *communicated* to others. Under our system of government, he can never be *compelled to express* them (except when upon the witness stand); and even if he has chosen to give them expression, he generally retains the power to fix the limits of the publicity which shall be given them.[36]

Although this interpretation of privacy along the lines of access control was adhered to for a long time, in times of global data flows and invisible data transfer, a control-based paradigm such as this has increasingly lost persuasive power.[37] The communication architecture of social networks alone is so entangled that users can hardly ever have complete control over the dissemination of their own personal data.[38] The networked infrastructure of digital communication and social relationships has made it necessary to reconsider a narrow individualistic conception of privacy. Ironically, it is the process of digitalization which highlights privacy's social form and value and points to a tradition of interactionist theories of individual and social freedom. This is a far more complex argument than it seems at first glance, because, so far, it is unclear whether

[32] ANNABELLE LEVER, ON PRIVACY 1 (2012). As a hallmark of the liberal tradition, see the Rawlsian distinction between the "right" and the "good" in JOHN RAWLS, POLITICAL LIBERALISM (2005). *See also* JOHN STUART MILL, ON LIBERTY (David Bromwich & George Kateb eds., Yale University Press 2003). For more on classical contract theory, see JOHN LOCKE, TWO TREATISES ON GOVERNMENT, (BiblioBazaar Reproduction Series 2008). For the reception of this tradition, see BEATE RÖSSLER, THE VALUE OF PRIVACY (2004); ALAN WESTIN, PRIVACY AND FREEDOM (1970).

[33] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

[34] *Id.* at 195–97.

[35] *See* Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 428–36 (1980).

[36] Warren & Brandeis, *supra* note 33, at 198 (emphasis added).

[37] However, the degree of complexity that a control-based understanding of privacy entails is already manifest in Warren and Brandeis' account. The communicative dimension of disclosure is in itself an inevitably *intersubjective* act of interaction with others, even when no actual communication takes place. It is the communicative relation with specific others that gives rise to different contexts of privacy. With reference to Warren and Brandeis, see Gusy, *supra* note 5, at 246.

[38] *See* Paula Helm & Sandra Seubert, *Normative Paradoxes of Privacy: Literacy and Choice in Times of Data Governmentality*, 18 SURVEILLANCE & SOC'Y (2020); Alice E. Marwick & Danah Boyd, *Networked Privacy: How Teenagers Negotiate Context in Social Media*, 16 NEW MEDIA & SOC'Y 1051 (2014).

https://doi.org/10.1017/glj.2020.101 Published online by Cambridge University Press

only privacy's societal and technological environment has changed or its conceptual understanding as well. There might well be core principles of a social understanding of privacy that historically exceed the digital age.[39] Although digitalization *per se* does not necessarily lead to a conceptual shift of privacy in general, we take this point one step further by arguing that the classical paradigm of individual control has not only lost its explanatory power, but also its normative power.[40]

Building on intersubjective approaches, a social understanding of privacy is evolving that challenges the fundamental assumptions upon which an individualistic conception is founded by emphasizing privacy's invariably social character.[41] Here, privacy itself is not only socially determined, but also functionally necessary for social relationships. According to this interpretation, beyond the realization of individual freedom, privacy is simultaneously a key prerequisite for achieving collective, or social, freedom.[42] In this respect, privacy acquires a social value that exceeds its importance for individuals. In the next section, we will provide a brief justification of the social value of privacy, before using these considerations as the basis for deriving a notion of the democratic value of privacy.

I. The Social Value of Privacy

Against the background of this social understanding of the concept, privacy is not just considered as a relationship of interaction and, thus, a practice that is intrinsically social, it is also described as a social good, deemed to be crucially important to democratic societies.[43] Following Priscilla Regan, the social value of privacy can be understood in three ways. First, it can be regarded purely as a socially shared value, ("common value") to which members of society relate in one form or another.[44] Second, privacy can take the form of a collective value, which captures the interdependence between the privacy of each individual and the whole of society.[45] Here, the social value of privacy envisions that a socially accepted and effective protection of privacy is necessarily reliant on a context characterized by genuine mutual interest in reciprocal privacy protection. Consequently, privacy must be recognized by society; in other words, the defense of individual boundaries must be considered socially appropriate whilst their transgression by others must be perceived as a violation. Third, and finally, Priscilla Regan identifies privacy as a public value, which signifies privacy's constitutive importance for the success of democratic autonomy.[46]

[39]An alternative conceptual tradition, for example, refers to Hegel, who emphasizes the social importance of the private sphere—here, the family as a social institution of intimate social relationships—in its constitutive function for the autonomy and self-development of the individuals involved. *See* G.W.F. Hegel, Grundlinien der Philosophie des Rechts, Dritter Teil, erster Abschnitt, (Hangeorg Hoppe ed., Suhrkamp 2004). For a reinterpretation, see Axel Honneth, Das Recht der Freiheit (2011).

[40]*See* Philipp K. Masur, Situational Privacy and Self-Disclosure: Communication Processes in Online Environments (2019); Sandra Seubert, *Offenbarung und Kontrolle: Die soziale Dynamik des Privaten*, 35 Der Blaue Reiter 52 (2014).

[41]For a comprehensive overview, see Beate Rössler & Dorota Mokrosinska, Social Dimensions of Privacy (2015).

[42]*See* Carlos Becker, *Privatheit und kommunikative Freiheit im Internet*, *in* Politische Theorie und Digitalisierung 45, 53–56 (Daniel Jacob & Thorsten Thiel eds., 2017).

[43]*See* Kirsty Hughes, *The Social Value of Privacy: The Value of Privacy to Society and Human Rights Discourse*, *in* Social Dimensions of Privacy, *supra* note 41, at 225; Valerie Steeves, *Reclaiming the Social Value of Privacy*, *in* Privacy, Identity and Anonymity in a Network World: Lessons from the Identity Trail 191 (Ian Kerr et al. eds., 2009); Marwick & Boyd, *supra* note 38. *See also* Irwin Altman, The Environment and Social Behavior: Privacy, Personal Space, Territory, Crowding 23–24 (1975).

[44]*See* Priscilla M. Regan, *Privacy and the Common Good: Revisited*, *in* Social Dimensions of Privacy, *supra* note 41, at 50, 56–60.

[45]*See* Priscilla M. Regan, Legislating Privacy: Technology, Social Values, and Public Policy 227–30 (1995).

[46]*Id.* at 225–27. As Regan makes clear, in most interpretations the "public value of privacy is derived from its importance to the exercise of rights that are regarded as essential to democracy, such as freedom of speech and association, and from its importance as a restraint on arbitrary power of government. But does privacy itself have an independent value to the political

https://doi.org/10.1017/glj.2020.101 Published online by Cambridge University Press

Here, *constitutive* is understood as meaning that a particular practice or institution is functionally necessary for the success of social relationships. In this vein, Beate Rössler and Dorota Mokrosinska describe privacy as a constitutive prerequisite for the existence of social roles, which can largely be distinguished by the degree of privacy communicatively displayed within them. Only when the degree of privacy is respected and recognized by the different interacting partners or social environments can specific roles become structurally consolidated and continue to exist.[47] Focusing on social contexts, Helen Nissenbaum has described in similar terms how a violation of contextually determined privacy and informational norms can damage these contexts as a whole.[48] The violation of established and widely accepted privacy norms can result in dysfunctional social relationships and social interaction contexts;[49] "norms of privacy are constitutive of social relationships."[50] But how, in this sense, can privacy be understood as a constitutive prerequisite for democracy?

II. Privacy and Democracy—A Tense Relationship

The democratic value of privacy is not self-evident. Indeed, democracy and privacy are often considered opposites, the fundamental normative principles of which—participation and transparency versus concealment and retreat, respectively—are perceived as incompatible.[51] Of course, this interpretation depends very much on how both concepts are defined—a discussion that has its own conceptual and political history.[52]

Nevertheless, for various reasons, both liberal and republican notions of democracy find it hard to assign privacy any kind of autonomous democratic value; the former due to its focus on individual rights, the latter due to its suspicion against any retreat from the public. Similarly, attempts to determine the political value of privacy negatively—through its antipodal position to the public sphere—are not of much help either, if the political value of privacy is ultimately taken to consist in its *not* being political.[53] Here, from the perspective of political liberalism, privacy acquires political value only *ex negativo* as the private is kept away from the political which, in turn, strengthens the latter.[54]

system?" *Id.* at 226. In her answer, Regan points to Hannah Arendt´s political understanding of privacy's *essential* contribution to the well-being of political communities by ensuring non-political spheres of human existence.

[47]Beate Rössler & Dorota Mokrosinska, *Privacy and Social Interaction*, 39 PHIL. & SOC. CRITICISM 771, 779–84 (2013).

[48]HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 129–50 (2010).

[49]This defense of "contextual integrity" might seem irritating, given the fact that the deconstruction of traditional privacy norms is central for feminist political thought and struggles. For a summary, see Judith Wagner DeCew, *The Feminist Critique of Privacy: Past Arguments and New Social Understandings*, *in* SOCIAL DIMENSIONS OF PRIVACY, *supra* note 41, at 85, 99–101. Nissenbaum's defense of privacy norms indeed has a potentially conservative bias in this respect. *See* Marcel Becker, *Privacy in The Digital Age: Comparing and Contrasting Individual Versus Social Approaches Towards Privacy*, 21 ETHICS & INFO. TECH. 307 (2019); Maria Brincker, *Privacy in Public and the Contextual Conditions of Agency*, *in* PRIVACY IN PUBLIC SPACE: CONCEPTUAL AND REGULATORY CHALLENGES 64, 68 (Tjerk Timan et al. eds., 2017) ("It seems that Nissenbaum with the descriptive notion precludes a normative critique of what has become the new normal.").

[50]Rössler & Mokrosinska, *supra* note 47, at 779. It is not only the loss of public anonymity due to the surveillance of public spaces with CCTV cameras, automated facial recognition, and the mass storage of digital communication data that is problematic from this perspective. The mixing of work and leisure, as well as economic, cultural, and exclusively private interests in social networks can similarly result in a sense of structural uncertainty in social contexts and role identities, as well as drain the potential for freedom released by privacy. *See* Sandra Seubert & Carlos Becker, *The Culture Industry Revisited: Sociophilosophical Reflections on "Privacy" in the Digital Age*, 45 PHIL. & SOC. CRITICISM 930 (2019).

[51]*See* AMITAI ETZIONI, THE LIMITS OF PRIVACY 187–98 (1999); Annabelle Lever, *Privacy Rights and Democracy: A Contradiction in Terms?*, 5 CONTEMP. POL. THEORY 142 (2006).

[52]*See* Sandra Seubert, *Das Vermessen Kommunikativer Räume: Politische Dimensionen des Privaten und ihre Gefährdungen*, 30 FORSCHUNGSJOURNAL SOZIALE BEWEGUNGEN (SCHWERPUNKTHEFT: PRIVATHEIT UND DEMOKRATIE) 124 (2017).

[53]*See* Dorota Mokrosinska, *Privacy and the Integrity of Liberal Politics: The Case of Governmental Internet Searches*, 45 J. SOC. PHIL. 369 (2014).

[54]A similar interpretation of privacy can also be formulated from a neo-republican perspective taking an anti-authoritarian approach. By protecting privacy from potential interference, predominantly by political institutions, certain forms of political

https://doi.org/10.1017/glj.2020.101 Published online by Cambridge University Press

We must ask, however, whether privacy should, as in this case, be considered solely instrumentally as a necessary counterpart to liberal political systems, or rather be described as a sufficient condition for a more successful practice of democratic self-determination, perhaps even as a constitutive element of democracy itself. In the former case, privacy is defined as an important but not essential resource for democratic societies—a lifeworld reservoir containing a plurality of opinions and life plans that constitute the "communicative underpinning"[55] of vibrant democracies and help them to thrive.[56] Here, privacy not only provides fertile ground for individuals capable of political action, but also fosters the development of political opinions and social interests, without the articulation of which democratic institutions would wither from the inside. According to this interpretation, privacy is an undeniably important aspect of diverse democratic societies. However, it is not functionally necessary for the achievement of democratic self-determination itself.

It is precisely this constitutive dimension of privacy which can now be exploited by conceptually linking privacy and democracy via an idea of communicative freedom based on a social theory of intersubjectivity. Of course, how we determine the democratic value of privacy, again, ultimately depends on what conception of democracy we presuppose. A normative definition of democracy grounded on the idea of unrestricted and equal communication is, in fact, not self-evident. It can, however, fall back on a broad spectrum of theories of democracy which draw on the concept of deliberation and hence in the broadest sense pertain to the idea of communicative freedom and discursive rationality. Deliberative theories of democracy characterize free and equal acts of communication between individuals as being simultaneously democratic *and* rational. Precisely because every potential participant can take part in a process of democratic self-determination by performing free acts of communication, we can expect reasonable processes of argumentative exchange to produce rational communicative results. Democratic institutions could provide and promote this very infrastructure of deliberative exchange by guaranteeing the maximum possible level of unrestricted communication. Communicative freedom, however, is not exhausted by participation in the institutionalized procedures of democratic practice.

Following Jürgen Habermas and Klaus Günther, communicative freedom could be given a two-pronged understanding comprised of the voluntary communication of each individual and the collective freedom of a communication community.[57] The crucial point here is that, from the perspective of a discourse theory of democracy, these two dimensions of communicative freedom should be treated as interwoven and co-original; individual communicative freedom can ultimately only be achieved in a context characterized by a mutual interest in facilitating, protecting, and realizing this freedom for everybody else. A free communication community, in turn, depends on the individual communicative freedom of its members, albeit a freedom to which it cannot be reduced.[58] Habermas, in particular, translated this "co-originality"[59] of communicative autonomy into a discourse-theoretical understanding of the law, according to which the legal procedures of collective democratic self-determination and individual civil liberties are mutually interdependent and legitimize one another. In this sense, individual civil liberties which aim to facilitate private

rule are quasi-instrumentally ruled out by privacy, such that the democratic character of political systems is strengthened. *See* Andrew Roberts, *Why Privacy and Domination?*, 4 Eur. Data Protection L. Rev. 5, 8–11 (2018). *See also* Andrew Roberts, *A Republican Account of the Value of Privacy*, 14 Eur. J. Pol. Theory 320, 336–38 (2015); Andrew Roberts, *Privacy, Data Retention and Domination: Digital Rights Ireland Ltd v Minister for Communications*, 78 Mod. L. Rev. 535 (2015); Regan, *supra* note 45, at 225–26.

[55]Sandra Seubert, Kommunikatives Unterfutter: Über die Bedeutung privater, Räume 964 (2014).

[56]*See* Daniel J. Solove, Understanding Privacy 91–94 (2008).

[57]*See* Jürgen Habermas, Between Facts and Norms (1996); Klaus Günther, *Communicative Freedom, Communicative Power, and Jurisgenesis*, 17 Cardozo L. Rev. 1035 (1996).

[58]For a similar interpretation, see Christopher Parsons, *Beyond Privacy: Articulating the Broader Harms of Pervasive Mass Surveillance*, 3 Media & Comm. 1 (2015).

[59]Habermas, *supra* note 57, at 127.

https://doi.org/10.1017/glj.2020.101 Published online by Cambridge University Press

autonomy are also interwoven with an idea of political autonomy realized via democratic collective liberties.[60]

From this perspective, communicative autonomy and fundamental rights are inseparable. Habermas clearly demonstrates that communicative freedom can be realized in an egalitarian manner only if it is founded on fundamental rights that are equally accessible and used in a non-strategic way—a way that refers to a communicative rationality of mutual understanding. Consequently, strengthening fundamental rights can contribute to an increase in communicative freedom at both an individual and collective level. To be clear, these fundamental rights *per se* do not fulfill the ideal of communicative freedom—as individual rights they could even have the opposite effect[61]—but they are institutionalized preconditions of communicative autonomy and equality and thus open up a space for communicative freedom's potential emergence. By doing so, they underpin the anarchic processes of societal communication with a constitutive framework, which the former cannot guarantee to provide in its dynamic and fluent character. Only against this background could the strengthening of fundamental rights support an increase in communicative freedom.

But how can privacy be categorized in this context? On the one hand, the claim to privacy can be understood as a communicative retreat, or "dropping out,"[62] of communicative obligations, something which initially appears to be diametrically opposed to the idea of democracy. Here, communicative freedom would simply comprise the right to non-communication.[63] On the other hand, if privacy is defined by the context and interaction-dependent delineation of communicative disclosure or concealment, then communicative freedom consists in the legally protected, unforced opportunity to be able to decide for oneself where and to whom information is revealed.[64]

Communicative demarcations are never simply the product of a single individual's decision, however. They always depend on the external social and legal circumstances, which react to these boundaries in different ways. Individual boundaries can be respected or violated, recognized or abused. This applies equally to intimate and professional as well as political and public relationships. Individual communicative freedom as an autonomous decision about what, how, and with whom a person wishes to communicate depends on a communication community that, as far as possible, respects these expectations and interactive relationships which normatively embed a specific approach to privacy. It is particularly these types of individual or collective demarcations that encounter enormous obstacles due to digital transformation. Economic actors in search of raw, preferably authentic, communication data expect monetary advantages from penetrating or circumventing these boundaries. In addition, political organizations and intelligence services, as well as insurance and utility companies, also have a keen interest in "transparent" citizens in order to produce the most precise forecasts and risk assessments possible.

Indeed, these citizens' individual delineations can themselves become the object of observation: who enters into what social relationships, with whom, and why is not only forming part of intelligence metadata and mass surveillance, but also becoming increasingly important for others, such

[60]*Id.* at 82–131.

[61]There is an unavoidable tension in the realization of communicative freedom through the form of law which cannot be extensively discussed here. Habermas himself realizes the problem when pointing out that its spontaneity cannot be legally enforced but can only be assumed—regenerating itself from a society's liberal traditions and associations of a liberal political culture. *See id.* at 164–65. For a further discussion of privacy rights´ dialectical relation to personal and societal freedom from a Critical Theory point of view, see Seubert & Becker, *supra* note 50.

[62]Habermas, *supra* note 57, at 120.

[63]*Id.* at 119–20.

[64]*See also* Carlos Becker & Sandra Seubert, *Privatheit, kommunikative Freiheit und Demokratie*, 40 Datenschutz und Datensicherheit 73 (2016).

https://doi.org/10.1017/glj.2020.101 Published online by Cambridge University Press

as marketing companies and political campaigning organizations.[65] Here, too, the asymmetrical configuration of the digital communication landscape and its actors can contribute to the erosion of a socially shared and thus protected practice of privacy, which also negatively influences the communicative freedom of each individual.

Initially, however, this merely demonstrates that privacy can be understood as a social relationship which is mutually dependent on the wishes of individuals and the socio-political structures around them. The constitutive significance of privacy—understood as a process of communicative concealment and disclosure—for the democratic practice of self-determination comes to light only when it becomes evident, say on the basis of discourse theory, that the autonomous demarcation of boundaries regarding where, with whom, and what an individual wishes to share can be viewed as the expression of individual communicative freedom, on which democracies fundamentally depend. Insofar as we follow deliberative theories in conceiving democracies as liberal structures of communicative self-determination, democracy's normative promise is grounded on the precondition that its members are entitled, first, to communicate on both a free and equal basis and, second, to make their own decisions about the manner and extent of their external communication.

Furthermore, it is precisely this that can be understood as a component of privacy, because it implies decisions about where and to whom individuals reveal information and to whom they do not. The democratic value of privacy derived in this way is rooted in the fact that privacy is an enabling condition for communicative autonomy which, in turn, not only calls for respect from political institutions, but also forms an essential part of democracy's promise of freedom. Indeed, a concept of a democracy where citizens are not permitted to decide independently what, how, and to whom they wish to communicate is simply absurd.

It is precisely this connection that is disrupted on a huge scale by the mass surveillance of digital communication and its increasing commodification. As discussed earlier, these practices blur established privacy norms in a partly illegitimate manner[66] and interfere with the basic functional structures of social relationships. Indeed, they fundamentally challenge the normative promise of communicative freedom upon which democracies are constitutively grounded. Here, commodifying communication and rendering it a policed or even involuntary action in a state of uncertainty affects the very essence of free communication as the basis of democratic practice.[67]

Clearly, as Hannah Arendt was already aware of, each act of communication is a leap of faith and ultimately has a relatively uncontrollable life of its own.[68] Moreover, digital communication is necessarily only indirectly possible as it always operates via an infrastructure provided by private third parties. These structural characteristics of the internet, however, must be separated from power asymmetries that are entailed by intelligence and economic practices of surveillance and commodification. In many cases such as this, the violation of privacy and communicative autonomy is already made manifest at the very start of a communication or is even taken as its prerequisite. After all, this can already be seen with regard to services and apps offering social networking supposedly free of charge, but which actually make users pay with their communication data.[69]

[65]On the latter, see Colin Bennett, *Trends in Voter Surveillance in Western Societies: Privacy Intrusions and Democratic Implications*, 13 Surveillance & Soc'y 370 (2015).

[66]This is not to deny the possibility of emancipatory effects that can also be associated with the erosion of certain contexts and privacy norms.

[67]*See* Beate Rössler, *Should Personal Data be a Tradable Good? On the Moral Limits of Markets in Privacy, in* Social Dimensions of Privacy, *supra* note 41, at 141; Shoshana Zuboff, The Age of Surveillance Capitalism (2019); Titus Stahl, *Indiscriminate Mass Surveillance and the Public Sphere*, 18 Ethics & Info. Tech. 33 (2016); Parsons, *supra* note 58; Roberts, *A Republican Account of the Value of Privacy, supra* note 54.

[68]*See* Hannah Arendt, Vita activa oder Vom tätigen Leben (9th ed. 2010).

[69]Sebastian Sevignani emphasized this further by referring to the existential necessity of participating in practices of digital communication, describing them as decisive for the visibility of and participation in social life and work practices. Drawing on

https://doi.org/10.1017/glj.2020.101 Published online by Cambridge University Press

We must be careful, however, not to conflate communicative freedom with political freedom of expression, which is also part of communicative freedom. After all, our main focus here concerns communicative demarcation lines drawn by individuals with regard to their privacy. In this sense, the collective freedom of democratic self-determination qua liberal communication can be achieved only if all members of the democratic communication community are given guarantees that they are allowed to decide autonomously what they want to reveal, to whom, and in what context. From this perspective, coerced, involuntary, and de-contextualized communication can be perceived not only as infringing each affected individual's communicative autonomy, but also as damaging a collective, liberal practice of communication, which is at the very heart of functioning democratic societies. In this sense, legal guarantees that protect an individual's private life and private acts of communication should, therefore, be understood as more than just increasing the freedom of each individual. Rather, given that these legal guarantees grant the right to protection to individuals with regard to their communicative autonomy, we also need to explore their fruitful influence on democracy. It is the legal protection of personal privacy which, by protecting the communicative autonomy of individuals, contributes simultaneously to the preservation as well as expansion of a democratic communication community and to the practice of collective communicative autonomy which, in turn, can be identified as the essential core of well-performing democratic societies. Therefore, defending privacy based on a communicative theory of democracy also identifies protection of the fundamental right to privacy as a key prerequisite for achieving communicative autonomy. As such, the democratic value of strictly interpreting the fundamental right to privacy becomes evident.

D. Conclusion: The Impact of Protecting European Fundamental Rights on Democratic Practices

Given our reflections drawn from theories of democracy in the previous section, it becomes evident that the prevailing threats to privacy—that is, to personal information and communicative relationships—emanating from economic and state actors are not just problematic in regard to individual freedom. Over and above that, invisible and unsolicited disclosure together with storage and analysis of private communication data, as well as online interactions, also prove to be a fundamental infringement upon the realization and possibilities for realization of democratic freedom. By damaging the communicative autonomy of individuals, democratic society as a whole, built on the foundations of free communication, is also damaged.

While focusing on the collective and public value of privacy, which, as set out by Priscilla Regan, draws attention to the reciprocity and general usefulness of individual privacy, effective and reliable protection of each individual's communicative freedom remains a fundamental condition of democratic freedom. As discussed above, an individual's fundamental right to privacy, which explicitly includes communicative relationships, thus also plays a pivotal role in the interpretation of privacy based on intersubjectivity and discourse theory. Against this backdrop, it is not just the rule of law's implementation that requires privacy protection to be defended as a fundamental right. Defense is also required for the normative obligations connected with a deliberative principle of democracy, which dovetails the realization of individual and collective freedom with the concept of communicative autonomy.

It is exactly this dovetailing which prompts us to explore the potential impact on democratic practice that might be brought to bear by protecting the fundamental right to privacy as promoted by the CJEU. The central role that European primary law and the CJEU assign to a fundamental right to privacy, together with the significance that has been attached to data protection through

Marx, he calls this the *double freedom of the Internet user*. *See* Sebastian Sevignani, *Zur Dialektik von Privatheit und Überwachung im informationellen Kapitalismus*, *in* Kritische Öffentlichkeiten. Öffentlichkeiten in der Kritik 237, 249–51 (Kornelia Hahn & Andreas Langenohl eds., 2017).

https://doi.org/10.1017/glj.2020.101 Published online by Cambridge University Press

the GDPR in European secondary law, are not the only evidence for a more effective rule of law and stronger individual civil rights. Rather, the protection of individual privacy rights is also eminently important for democracy, because such rights can be interpreted as a prerequisite for the realization of democratic freedom. As such, privacy can also be understood as a collective good, which accordingly, for its protection, calls not just on each individual, but also the democratic community as a whole. This ultimately also obliges political and state institutions to improve the protection of democratic societies' communicative infrastructure in light of the new challenges and threats presented by the digitalization of our everyday life. Therefore, to understand privacy also as a collective or public good implies that different political strategies are needed in order to address these challenges.

The social understanding of privacy underlying these considerations can thus be reformulated as a positive duty to strengthen the systematic protection of privacy by public means so as to relieve individuals from the task of protecting their own privacy. From a legal science perspective, this shift in perspective could necessitate a partial departure from a notion of privacy protection that understands this concept exclusively in the language of liberal rights. The positive duty to protect privacy as a collective and public good could, for instance, be translated here as an obligation on the part of political and legal institutions to render users' established trust in communication infrastructures itself into an object of protection.[70] The collective trust in communicative network structures can, of course, be protected only if these are kept strictly in check by institutions and fundamental rights, as well as being controlled by politics and civil society. Thus, protecting privacy as a public good also proves in practice to be a collective responsibility in democratic societies. Although this is not limited to law, it is significantly underpinned by it.

The protection of individual privacy as a fundamental right, particularly as applied to private communication in the digital space and as advanced by the CJEU, can thus be clearly identified as a contribution to protecting the democratic value of privacy under the new conditions of digital surveillance and commodification. In this sense, the strengthening of European privacy protection can at the same time be understood as the strengthening of European democracy.

Exactly how democracy might be strengthened through European privacy protection is certainly an appropriate subject for future research, especially within political science. Particularly from the perspective of democratic theory, the relationship between privacy rights, EU citizenship, and digital market economy interests will play a crucial role in any future inquiries into the challenges posed by digital transformation in Europe. Ultimately, any debate on this topic will have to focus on the fundamental relationship of democratic civil liberties with economic and security interests, which via privacy protection affects the very essence of democracy itself.

[70]Pertinent to this, see Johannes Eichenhofer, *Privatheit im Internet als Vertrauensschutz: Eine Neukonstruktion der Europäischen Grundrechte auf Privatleben und Datenschutz*, 55 Der Staat 41 (2016). *See also* Woodrow Hartzog, Privacy's Blueprint: The Battle to Control the Design of New Technologies (2018); Eichenhofer, *supra* note 5.

Cite this article: Seubert S, and Becker C (2021). The Democratic Impact of Strengthening European Fundamental Rights in the Digital Age: The Example of Privacy Protection. *German Law Journal* **22**, 31–44. https://doi.org/10.1017/glj.2020.101