Data Protection by Design? A Critique of Article 25 of the GDPR

Ari Ezra Waldman†

Europe's General Data Protection Regulation (GDPR) took effect on May 25, 2018. Article 25, titled, "Data Protection by Design and by Default," purports to incorporate the concept of "privacy by design" into European data protection law. This Article challenges that common presumption. Although privacy by design is not a new doctrine, having been the subject of academic debate, legal, and regulatory discussions for more than a decade, the final draft of Article 25(1) reflects little, if any, of that history. Relying on multiple forms of statutory interpretation commonly used to interpret European Community legislation, this Article argues that Article 25 of the GDPR lacks any meaningful connection to privacy by design under textualist, contextual, purposive, and precedential interpretations. Only teleological reasoning offers a meaningful way forward. This means that it is up to the European Court of Justice to determine if Article 25(1) will have any chance of protecting European Union citizens and limiting the power of data controllers.

† Professor of Law and Computer Science, Northeastern University School of Law and Khoury College of Computer Sciences. Visiting Professor, Woodrow Wilson School of Public and International Affairs, Princeton University (2019-2020). Affiliate Fellow, Information Society Project, Yale Law School. Ph.D., Columbia University; J.D., Harvard Law School. Thanks to Kendra Alpert, Michael Birnhack, Lee Bygrave, Danielle Keats Citron, Mary Culnan, Nico van Eijk, Sue Glueck, Woodrow Hartzog, Mike Hintze, Meg Leta Jones, Cameron Kerry, Jonathan Mayer, Sean McDonald, Neil Richards, Ira Rubinstein, James Rule, Stuart Shapiro, Felix Wu, and Tal Zarsky for their helpful and insightful comments. Portions of this Article are taken from my article, *Privacy's Law of Design*, 9 U.C. IRVINE L. REV. 1239 (2019). Versions of this Article were presented or workshopped at the AI and the Law Conference at Seton Hall University School of Law, at the Privacy Law Scholars Conference in Washington, D.C., and at the Berlin Center for Consumer Policies Annual Forum in Berlin, Germany. Special thanks to the editors at the *Cornell International Law Journal*. All errors are my own.

Introduction

When the General Data Protection Regulation (GDPR) took effect on May 25, 2018, "data protection by design and by default" became the law of the European Union.[1] The concept, embodied in Article 25, Section 1, requires a data "controller" to

> both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.[2]

This provision is far from clear. This Article leverages a variety of statutory interpretation methods commonly used to interpret European statutory law to discern what Article 25 actually means.[3] It concludes that Article 25(1) is hopelessly vague. Neither the text nor its context offers any clarity about Article 25(1)'s requirements, scope, or limitations. Only a teleological approach can rescue Article 25(1) from obscurity and obsolescence.

Most scholars and industry experts suggest that Article 25(1) codifies privacy by design into law. Daniel Solove has stated that "Article 25 . . . mandates that data protection be built in starting at the beginning of the design process,"[4] reflecting one of the standard academic definitions of privacy by design. Woodrow Hartzog wrote that Article 25, which "requires that core data protection principles be integrated into the design and development of data technologies," is important because privacy by design is an essential weapon in vindicating privacy rights against predatory, data-hungry technology companies.[5] The international consulting firm Deloitte told its clients that "privacy by design" was "new as a legal requirement under" Article 25, requiring companies to embed privacy in the design process.[6] And PrivacyTrust called Article 25 a "key change[ ]"

---

1. *See* Council Regulation 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) 15, 65 (EU) [hereinafter GDPR].

2. *Id.* at art. 25(1).

3. *See generally* Koen Lenaerts & José A. Gutiérrez-Fons, *To Say What the Law of the EU Is: Methods of Interpretation and the European Court of Justice*, 20 COLUM. J. EUR. L. 3 (2014). This Article focuses almost exclusively on Section 1 of Article 25 because Section 1 is widely understood to codify privacy by design. Section 2, which covers privacy "by default," is discussed more briefly because there is less history, context, and background scholarship to address. Notably, there is similar confusion about the meaning of Section 2.

4. Daniel J. Solove, *Why I Love the GDPR: 10 Reasons*, PRIVACY + SECURITY BLOG (May 2, 2018), https://teachprivacy.com/why-i-love-the-gdpr/ [https://perma.cc/679H-DPPV].

5. WOODROW HARTZOG, PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES 54 (Harvard Univ. Press 2018).

6. Shay Danon, *GDPR Top Ten: #6: Privacy by Design and by Default*, DELOITTE (Feb. 10, 2017), https://www2.deloitte.com/nl/nl/pages/risk/articles/gdpr-top-ten-6-privacy-by-design-and-by-default.html [https://perma.cc/99YA-X4N5].

that "provides the recognition of [the right to privacy by design] and how it is to be enforced."[7]

There are two problems with that neat narrative, both of which I describe in this Article. First, although the phrase "privacy by design" generally refers to making privacy part of the design process for new technologies, scholars have long disagreed about what that actually means, making it difficult to codify it as a unitary concept.[8] Second, the very diversity of definitions means that the drafters of the GDPR had several choices: they could have codified one version, tried to blend different definitions together, developed another perspective entirely, or used language so vague that the provision would be rendered meaningless. Article 25(1) reflects the last option, comprising language so devoid of meaning that it can hardly be considered to reflect privacy by design at all. I argue that under most methods of statutory interpretation used by the Court of Justice of the European Union (CJEU or Court of Justice), Article 25(1) does not reflect privacy by design. Rather, it was written as a catch-all provision that has no identity of its own. The CJEU will have to leverage teleological reasoning to empower the provision. If it does not, European citizens will have lost what could be a powerful tool of data protection.

I. What is "Privacy by Design"?

Privacy by design has a long, diverse paper trail. Indeed, even before the GDPR, the growing literature included six different approaches to privacy by design. The GDPR's language does not incorporate any of these approaches into design law. This Part teases out these varied definitions, thus describing the context in which Article 25 was written.

1. *The FIPPs.* Definitions of privacy by design have always started with the Fair Information Practice Principles (FIPPs), which developed out of a 1973 report from the United States Department of Housing, Education, and Welfare (HEW).[9] The HEW Report recommended that users be informed of data use practices, have the opportunity to correct their data, and consent to any secondary uses of their information.[10] The report also called on companies to be transparent about their data use practices, set limits on what data they gather and process (also known as data minimization), include sunsets for data retention, and maintain appropriate levels of security for any stored data.[11] Some of these same principles—data minimization, access, transparency, and, particularly, consent—are embedded in the GDPR. Indeed, Article 25 lists "data minimisation" as a governing

7. *Privacy by Design GDPR*, PRIVACY TR., https://www.privacytrust.com/gdpr/privacy-by-design-gdpr.html [https://perma.cc/L3XW-XG49] (last visited July 9, 2018).

8. *See* discussion *infra* Part I.

9. *See generally* U.S. DEP'T OF HEALTH, EDUC. & WELFARE, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS: REPORT OF THE SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS (1973).

10. *Id.* at 41–42.

11. *Id. See also* Paul M. Schwartz & William M. Treanor, *The New Privacy*, 101 MICH. L. REV. 2163, 2181 (2003).

privacy principle.[12] And twenty-one other GDPR provisions make consent the shibboleth of privacy protection.[13] It would be easy, therefore, to see Article 25 as a recitation of the FIPPs.

2. *PbD*. The FIPPs are at the core of a second definition of privacy by design. When Ann Cavoukian, the former Information and Privacy Commissioner of Ontario, Canada, described her seven "foundational" principles of privacy by design, or PbD, she was either consciously or unconsciously relying on the FIPPs. The principles—Proactive not Reactive; Privacy as a Default Setting; Privacy Embedded into Design; Full Functionality; End-to-End Security; Visibility and Transparency; and Respect for User Privacy[14]—echo principles of user control and transparency that were in the HEW Report. And, as Ira Rubinstein and Nathaniel Good have argued, these principles are either repetitive (the first three principles are siblings, if not triplets) or so broad that they provide little additional guidance beyond the general notion that privacy by design is about "considering privacy issues early in the design process and setting defaults accordingly."[15]

3. *Promoting Consumer Privacy at the FTC*. The Federal Trade Commission (FTC) says that privacy by design refers to companies "promot[ing] consumer privacy throughout their organizations and at every stage of the development of their products and services."[16] On the ground, that has translated into requiring companies to adopt privacy programs that include design considerations. For example, in March 2011, the FTC required Google to "design and implement[ ] . . . reasonable privacy controls and procedures" in response to a privacy risk assessment.[17] It required the same of Facebook later that year.[18] But the FTC has never explained what that means in practice.

4. *Translating Privacy into System Requirements*. Rubinstein has related privacy by design to Privacy Enhancing Technologies (PETs), or engineering tools that translate specific data protection laws into code.[19] By way of example, Rubinstein and Good explain that privacy by design should

12. *See* GDPR, *supra* note 1, at art. 25.

13. *See id*. at arts. 4, 6–9, 22, 49. *See also id*. at 6–11, 14, 21, 29–31 (Specifically, recitals 32, 33, 38, 40, 42, 43, 50, 51, 54, 71, 111, 155, 161, and 171).

14. *See* Ann Cavoukian, *The 7 Foundational Principles: Implementation and Mapping of Fair Information Practices*, Privacy by Design 1, 6 (2010), https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf [https://perma.cc/D869-KUA7]; Ira S. Rubinstein & Nathaniel Good, *Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents*, 28 Berkeley Tech. L.J. 1333, 1337 (2013).

15. Rubinstein & Good, *supra* note 14, at 1338.

16. F.T.C., Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers 22 (2012) [hereinafter FTC Report].

17. Google, Inc., F.T.C. File No. 102 3136, at 5 (Mar. 30, 2011), https://www.ftc.gov/sites/default/files/documents/cases/2011/03/110330googlebuzzagreeorder.pdf [https://perma.cc/7QCL-GE83].

18. Facebook, Inc., F.T.C. File No. 092 3184, at 6 (Nov. 29, 2011), https://www.ftc.gov/sites/default/files/documents/cases/2011/11/111129facebookagree.pdf [https://perma.cc/3VFT-35P6].

19. *See* Ira S. Rubinstein, *Regulating Privacy by Design*, 26 Berkeley Tech. L.J. 1409, 1410, 1414–28 (2011). *See also* Rubinstein & Good, *supra* note 14, at 1341 ("privacy by

require companies not merely to promise to delete user data after a limited amount of time, but rather to design a database that automatically identifies personal information and deletes it at a pre-programmed date.[20] More broadly, Seda Gurses, Carmela Troncoso, and Claudia Diaz recognized that privacy encompasses more than just technical security requirements and captures the social concerns of discrimination, equality, and human flourishing. They have argued that privacy by design requires translating the "social, legal and ethical concerns" embraced by the concept of privacy "into systems requirements," or pieces of code to make a machine run.[21] They recommend starting from data minimization and, from that foundation, generalizing engineering principles to enhance privacy.[22]

5. *Organization*. Kenneth Bamberger and Deirdre Mulligan suggest that privacy by design includes organizational measures that integrate privacy professionals into a technology company's various business units.[23] Elsewhere, I have argued that companies need to go further, integrating lawyers and privacy professionals into design teams and acculturating designers themselves into the ethos of privacy and ethics in design.[24]

6. *Values, Principles, and Guidelines*. Hartzog has taken a significant step toward translating privacy by design into law. Going beyond the general conception that privacy by design refers to an *ex ante* approach to privacy, Hartzog calls for a design agenda that guides the design of technologies that affect our privacy. Through tort law, contract law, consumer protection law, and surveillance law, Hartzog calls on the law to "set boundaries and goals for technolog[y] design."[25] For example, a design agenda for privacy, Hartzog argues, would respond to the problem of "extracted consent"—or the way online platforms design interfaces, agreements, and click boxes to manipulate, nudge, and encourage us to acquiesce to a data-sucking regime—with an evolved contract law regime that considers the role of malicious interfaces in contract validity.[26] This important step in the ecosystem of privacy by design scholarship recognizes that better corporate behavior and the law must work together to create privacy-enhancing design.

---

design requires the translation of [privacy principles] into engineering and design principles and practices.").

20. Rubinstein & Good, *supra* note 14, at 1341–42.

21. Seda Gürses, et al., *Engineering Privacy by Design*, *in* COMPUTERS, PRIVACY & DATA PROTECTION 25 (2011).

22. *Id.* at 26.

23. *See* KENNETH A. BAMBERGER & DEIRDRE K. MULLIGAN, PRIVACY ON THE GROUND: DRIVING CORPORATE BEHAVIOR IN THE UNITED STATES AND EUROPE 76–86 (MIT Press 2015).

24. *See generally* Ari Ezra Waldman, *Designing Without Privacy*, 55 HOUS. L. REV. 659 (2018).

25. HARTZOG, *supra* note 5, at 7.

26. *Id.* at 211–13.

II. What is Article 25?

Where, if anywhere, does Article 25 sit among these diverse approaches to privacy by design? That is a question of statutory interpretation. European courts are tasked with ensuring that the European Union's (EU) treaties and legislation are faithfully interpreted and observed.[27] But the "European way" of interpreting statutes differs from the methods employed by courts in the United States (U.S.). The CJEU has stated that it interprets EU law "in accordance with generally accepted methods of interpretation, in particular by reference to the fundamental principles of the [EU] legal system and, where necessary, general principles common to the legal systems of the Member States."[28] As Lord Denning stated in *HP Bulmer Ltd. v. J. Bollinger SA & Ors*,[29] where legislation "lack[s] precision," American lawyers would look for language in the statute to help interpret the law's meaning.[30] European judges should "look to the purpose and intent . . . . They must divine the spirit . . . and gain inspiration from it. If they find a gap, they must fill it as best they can."[31] Lord Denning adopted this approach from Section 3(1) of the European Communities Act, which was passed by the United Kingdom's (U.K.) Parliament so the U.K. could join the EU.[32] The Act states that any question as to the meaning of a treaty, piece of legislation, or any other regulation—directive or instrument—must be treated "as a question of law" to be determined "in accordance with the principles laid down by and any relevant decision of the European Court."[33]

To do that, European courts tend to employ six methods of interpretation:[34] textual, purposive, historical, precedential, contextual, and teleolog-

27. Consolidated Versions of the Treaty on European Union and the Treaty Establishing the European Community, Dec. 24, 2002, 2002 O.J. (C 325) 124 [hereinafter EC Treaty].

28. Joined Cases C-46/93 & C-48/93, Brasserie du Pêcheur SA v. Bundesrepublik Deutschland and The Queen v. Sec'y of State for Transp. *ex parte* Factortame Ltd., 1996 E.C.R. I-01029, ¶ 27.

29. HP Bulmer Ltd. v. J. Bollinger S.A. & Ors [1974] 3 WLR 202.

30. *Id.*

31. *Id.*

32. The United Kingdom left the European Union on January 31, 2020. Nevertheless, the interpretive principles discussed in the European Communities Act remain sound. *See, e.g.*, *U.K. Leaves E.U., Embarking on an Uncertain Future*, N.Y. TIMES (Jan. 31, 2020), https://www.nytimes.com/2020/01/31/world/europe/brexit-britain-eu.html? [perma.cc/EF3M-D8QX].

33. European Communities Act, 1972, c. 68, § 3 (1) (U.K.), https://www.legislation.gov.uk/ukpga/1972/68/section/3 [perma.cc/9GBG-E2WP].

34. The European Court of Justice rarely has occasion to state which interpretive principle it uses in a given case. Nor is it limited to any particular approach, as it is free to choose which interpretive method best suits the case and the EU. *See* Lenaerts & Gutiérrez-Fons, *supra* note 3, at 5–6. This taxonomy of interpretive tools is based on: ANTHONY ARNULL, THE EUROPEAN UNION AND ITS COURT OF JUSTICE 607–33 (Oxford Univ. Press 2d ed. 2006); K.P.E. LASOK ET AL., JUDICIAL CONTROL IN THE EU: PROCEDURES AND PRINCIPLES 376–97 (Oxford Univ. Press 2004). The specific names given to each approach is based on the terminology used in both of these sources, but there is some disagreement among scholars about the appropriate names for each interpretive method. *Compare* Hannes Rösler, *Interpretation of EU Law*, *in* 2 MAX PLANCK ENCYCLOPEDIA OF

ical.[35] Although "plain language" interpretations are more common in the U.S. than in Europe, this Part starts there for three reasons.[36] First, European judges will often start with the words of a legal instrument even if ultimately deciding the case through another lens. Indeed, many CJEU cases begin with the "actual" or "express" wording of a Community act.[37] Second, where the wording of a Community law is clear, teleological, contextual, or purposive interpretations generally do not question or wildly depart from the plain meaning of the law.[38] Otherwise, there would be no certainty to any legal provision.[39] And, in some cases, applying the ordinary meanings to words used in community acts can answer an interpretive controversy.[40] Third, to the extent that the GDPR and Article 25 may serve as models for future regulation in the U.S.—where a statute's plain language is considered far more readily—the language used is relevant. I argue that under most interpretations, Article 25 is a broad, vague, almost-meaningless, catch-all provision that does not reflect the privacy by design literature. Article 25 is repetitive of other sections of the GDPR and has no identity of its own. Only a teleological approach, which gives the CJEU vast interpretive leeway, can rescue the provision.

EUROPEAN PRIVATE LAW 979, 979 (Jürgen Basedow et al. eds., Oxford Univ. Press 1st ed. 2012) (referring to "grammatical, systematic and purposive" approaches), *with* Lenaerts & Gutiérrez-Fons, *supra* note 3, *passim* (referring to textualism and contextualism).

35. *See* Lenaerts & Gutiérrez-Fons, *supra* note 3, at 6, 16–17, 37 (noting the "'classical methods of interpretation', namely literal interpretation, contextual interpretation [including both systematic and historical intent] and teleological interpretation."); Case C-399/11, Melloni v. Ministerio Fiscal, 2013 E.C.R. ¶ 39 (suggesting that European courts should look at the "wording, scheme and purpose," including legislative intent, of a directive). *See also* Winfried Brugger, *Concretization of Law and Statutory Interpretation*, 11 TUL. EUR. & CIV. L. F. 207, 232 (1996) (discussing the "*classical canon of interpretation*," including "grammatical (also called textual, semantic), systematic (contextual, structural), historical and teleological (purposive) interpretation.").

36. *See* Case 22/70, Comm'n v. Council, 1971 E.C.R. 264, ¶¶ 6–32. For in-depth discussions of the plain language canon in U.S. statutory interpretation, see generally David A. Strauss, *The Plain Language Court*, 38 CARDOZO L. REV. 651 (2016); John F. Manning, *Second-Generation Textualism*, 98 CALIF. L. REV. 1287 (2010); Jonathan T. Molot, *The Rise and Fall of Textualism*, 106 COLUM. L. REV. 1 (2006).

37. *See* Lenaerts & Gutiérrez-Fons, *supra* note 3, at 13–23. *See also, e.g.*, Case C-326/99, Stichting 'Goed Wonen' v. Staatssecretaris van Financiën, 2001 E.C.R. I-1631, ¶ 45 ("actual wording"); Case C-438/99, Jiménez Melgar v. Ayuntamiento de Los Barrios, 2001 E.C.R. I-6915, ¶ 50 ("actual wording"); Case C-376/98, Ger. v. Parliament and Council, 2000 E.C.R. I-8419, ¶ 83 ("express wording").

38. *See* Lenaerts & Gutiérrez-Fons, *supra* note 3, at 9. *See also, e.g.*, Case C-48/07, Belg. v. Les Vergers du Vieux Tauves SA, 2008 E.C.R. I-10627, ¶ 44; Case C-263/06, Carboni e Derivati Srl v. Ministero dell'Economia e delle Finanze and Riunione Adriatica di Sicurtà SpA, 2008 E.C.R. I-1077, ¶ 48; Case C-220/03, European Cent. Bank v. Fed. Republic of Ger., 2005 E.C.R. I-10595, ¶ 31.

39. *See, e.g.*, Case C-582/08, Comm'n v. U.K., 2010 E.C.R. I-7195.

40. *See, e.g.*, Case 152/84, M. H. Marshall v. Southhampton and South-West Hampshire Area Health Auth., 1986 E.C.R. 723, ¶ 48 (stating that the directive at issue was not binding on individuals because Article 189 of the EC Treaty only states that directives are binding on "Member States"); Case 59/85, Neth. v. Reed, 1986 E.C.R. 1283 (holding that Article 10(1) of a regulation that gave the "spouse" of a migrant worker the right to live in the territory of the host State did not extend to unmarried partners).

A. Textual, or Plain Language, Interpretation

The plain language of Article 25 transforms privacy by design into nothing. The provision is constructed in three parts. First, it allocates responsibility to data collectors. Article 25, Section 1 states that a "controller shall" follow its requirements.[41] And, by controller, the GDPR means those that collect and analyze our data. A "controller" is one who "determines the purposes and means of the processing of personal data."[42] Second, Article 25(1) lays out a timeline for compliance. Its obligations arise twice: first, "at the time of the determination of the means for processing," or when the company is creating the tool that collects and analyzes personal data; and, second, "at the time of the processing itself," or when consumer data is being processed in the real world.[43]

The clarity ends there. Article 25(1) states that data controllers have to "implement appropriate technical and organisational measures such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner."[44] Stripping out the example clauses, Section 1 boils down to a requirement that data collectors "implement data protection principles . . . in an effective manner,"[45] or, in other words, adequately comply with the rules laid out elsewhere in the GDPR.[46] This language not only fails to specify what data collectors must do in order to comply, but it also relegates Article 25 to a catch-all status, without any value-add of its own.

Notably, the GDPR is not exclusively an English-language document. The EU has twenty-four official languages, all of them equally valid,[47] and the CJEU generally interprets community acts in ways that are consistent across translations.[48] The CJEU can also consider the language in different translations to clarify ambiguities in one,[49] and sometimes those com-

41. *See* GDPR, *supra* note 1, at art. 25.

42. *Id.* at art. 4(7).

43. *Id.* at art. 25(1).

44. *Id.*

45. *Id.*

46. Specifically, in Article 5. *See id.* at art. 5(1)(a)-(f) (including the following principles: "lawfulness, fairness and transparency;" "purpose limitation;" "data minimisation;" "accuracy;" "storage limitation;" and "integrity and confidentiality.").

47. *See* Council Regulation 385/58, Determining the Languages to be Used by the European Economic Community, 1958 O.J. (385) 59, 59 (EEC) (last modified by Council Regulation 517/2013, Adapting Certain Regulations and Decisions by Reason of the Accession of the Republic of Croatia, 2013 O.J. (L 158) 1, 71 (EU)); *see also* Language Policy, EUR. UNION, https://europa.eu/european-union/abouteuropa/language-policy_en [https://perma.cc/R99L-8G4F] (last visited July 20, 2018). For examples of this principle in practice, please see Case C-283/81, CILFIT & Lanifico di Gavardo SpA v. Ministry of Health, 1982 E.C.R. 3415, ¶ 18; and Case C-29/69, Erich Stauder v. City of Ulm, Sozialamt (Social Welfare Office), 1969 E.C.R. 419, ¶ 3.

48. *See* Lenaerts & Gutiérrez-Fons, *supra* note 3, at 10; ARNULL, *supra* note 34, at 608.

49. *See, e.g.*, Case 30/77, Regina v. Bouchereau, 1977 E.C.R. 1999, ¶ 13 (comparing the different language versions of the text at issue).

parisons reveal mistakes.[50] That said, the German and French versions of Article 25 are just as unhelpful as the English.[51] In German, Section 1 refers to steps "*die dafür ausgelegt sind, die Datenschutzgrundsätze wirksam umzusetzen*," or steps that are designed to effectively implement data protection principles.[52] It adds "*und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen*," which translates to: include the necessary guarantees in the processing [of data] in order to comply with the requirements of this regulation."[53] In French, Article 25 also simply requires controllers "*à mettre en œuvre les principes relatifs à la protection des données*," or to implement the principles of data protection.[54] Both of these versions are roughly the same. Generally, that's a good thing: consistency across the EU's many languages ensures uniformity across the bloc.[55] In this case, the uniformity is problematic. The lack of any specificity as to what "data protection by design" means ensures that data controllers have few guideposts when trying to identify their obligations and data subjects have few ways of knowing when their rights have been violated.

B. Purposive Analysis

Textual analyses are usually insufficient, particularly where language is ambiguous.[56] When the text of a Community act is unclear, the CJEU will often turn to the underlying purpose of the statute.[57] Initially, the Court of Justice rarely considered the opinions of legislators and statements during debate,[58] or what American lawyers might call legislative history (*travaux préparatoires*).[59] As those resources have become better

50. *See* Jeroen Terstegge, *GDPR: Lost in Translation?*, IAPP PRIVACY PERSP. (May 1, 2018), https://iapp.org/news/a/gdpr-lost-in-translation/ [https://perma.cc/7XFP-7NXF] (referring to several cases, in and beyond data protection law, involving translation errors).

51. German and French are two of the EU's three "procedural" languages—namely, those languages in which the EU conducts its business. English is the third. I am proficient in German and a novice in French. For interpretation, I consulted native or fluent speakers who are also lawyers.

52. The GDPR is available in multiple languages. *See* EUROPA, https://op.europa.eu/en/publication-detail/-/publication/3e485e15-11bd-11e6-ba9a-01aa75ed71a1/language-en [https://perma.cc/4SAG-3H22] (last visited July 2018).

53. *Id.*

54. *Id.*

55. *See* Case C-295/95, The Queen v. Comm'r of Customs & Excise *ex parte* EMU Tabac SARL, The Man in Black Ltd., and John Cunningham, 1998 E.C.R. I-1605, ¶ 36 (referring to the need for uniform interpretation of Community law).

56. *See* Lenaerts & Gutiérrez-Fons, *supra* note 3, at 6–7, 9.

57. *See* Theodor Schilling, *Alec Stone Sweet's "Juridical Coup d'État" Revisited: Coups d'État, Revolutions, Grenzorgane, and Constituent Power*, 13 GERMAN L.J. 287, 299 (2012) ("the historical interpretation generally asks less for the ideas of the 'founders' which are seen as only the draughtsmen of the future constitution (although the *travaux préparatoires* certainly play a role in interpretation) but for the ideas of the legislator, i.e. in the case of a historically first constitution, the constituent power.").

58. Case C-2/74, Reyners v. Belg., 1974 E.C.R. 657, 665–66.

59. *See, e.g.*, NEIL MACCORMICK, RHETORIC AND THE RULE OF LAW: A THEORY OF LEGAL REASONING 134 (Oxford Univ. Press 2005); Robert A. Katzmann, *Statutes*, 87 N.Y.U. L.

maintained and as the body of European law has grown, the CJEU has increasingly relied on legislative history to determine a statute's original intent.[60]

This approach has its shortcomings. Legislation is the result of input and compromise from many different legislators, who may have different reasons for voting the same way.[61] Moreover, interpreting a law based on the intention of its drafters may ossify the law and impede its adaptation to social changes.[62] To avoid these problems, Article 253 of the Treaty Establishing the European Community (EC Treaty) requires that Community statutes state the "reasons on which they are based."[63] These reasons will almost always be in the statutory preambles or recitals. And the Court of Justice has relied on these statements before when conducting a purposive analysis.[64]

There are 173 recitals attached to the GDPR.[65] They range from noting that data protection is a fundamental right (Recitals 1 and 4) to emphasizing the power of the EU to adopt implementing legislation (Recitals 167–170).[66] The CJEU can use some of these recitals to better understand both the purpose of Article 25(1) and the GDPR, but none of them help Article 25 reflect privacy by design.

Recital 78, which is supposed to flesh out Article 25, notes that

> [w]hen developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications . . . .[67]

This is a poorly written sentence. The subject, predicate, and object are modified twice, first by a prefatory phrase—"when developing, designing, selecting and using . . ."—and then again by a different concluding phrase—"when developing and designing."

REV. 637, 661–82 (2012). *See also* Stephen Breyer, *On the Uses of Legislative History in Interpreting Statutes*, 65 S. CAL. L. REV. 845, 846 (1992); Lawrence M. Solan, *Private Language, Public Laws: The Central Role of Legislative Intent in Statutory Interpretation*, 93 GEO. L.J. 427, 453 (2005).

60. *See* Lenaerts & Gutiérrez-Fons, *supra* note 3, at 23–24.

61. *See* Giulio Itzcovich, *The Interpretation of Community Law by the European Court of Justice*, 10 GERMAN L.J. 537, 554–55 (2009). *See also* Conroy v. Aniskoff, 507 U.S. 511, 519 (1993) (Scalia, J., concurring).

62. *See* Lenaerts & Gutiérrez-Fons, *supra* note 3, at 28; Karin Frick & Soren Schonberg, *Finishing, Refining, Polishing: On the Use of Travaux Preparatoires as an Aid to the Interpretation of Community Legislation*, 28 EUR. L. REV. 149, 154 (2003).

63. EC Treaty, *supra* note 27, at art. 253.

64. *See, e.g.*, Joined Cases C-402/07 & C-432/07, Sturgeon v. Condor Flugdienst GmbH and Böck & Lepuschitz v. Air Fr. SA 2009 E.C.R. 716, ¶¶ 42–44 (interpreting a statute providing rules and compensation for delayed airline passengers in light of the law's recitals); Case 14/69, Markus & Walsh v. Hauptzollamt Hamburg-Jonas, 1969 E.C.R. 349, ¶¶ 8, 11.

65. GDPR, *supra* note 1, at 1-31.

66. *Id.*

67. *See id.* at 15.

Nor do the recitals add much to what Article 25 means in practice. Recital 78 includes a list of potential technical measures that might, if implemented, help a company comply with Article 25. But those measures—"minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, [and] enabling the controller to create and improve security features,"[68]—reflect requirements embodied in other sections of the GDPR, particularly Article 5.[69] Recital 156 applies to the processing of personal data for scientific or historical research and recommends that institutions take "technical and organisational" measures to ensure "data minimisation," or that data is used for the narrow purpose for which it was collected.[70] But Article 47 already requires data minimization as a binding corporate rule in all contexts.[71] Therefore, it is not clear what Article 25 is adding to the GDPR overall.

The purposes of the GDPR are manifold. It aims to contribute to "freedom, security and justice . . . economic and social progress . . . the strengthening and the convergence of the economies" within the EU, and "the well-being of natural persons."[72] While recognizing that data protection is not an absolute right,[73] the GDPR is also meant to ensure "a high level of" protection for personal data.[74] It wants to "ensure an equivalent level of protection of natural persons and the free flow of personal data throughout the Union."[75] These diverse, sometimes conflicting, purposes do little to clarify Article 25. We can read Article 25 to impose significant obligations on data controllers in light of the overarching goal of ensuring a "high level" of data protection but ensuring the free flow of information counsels against significant regulation that could hinder corporate use of data. In any event, this purposive approach does not specify corporate design obligations or data subject rights.

C. Statutory History

Of course, the GDPR did not emerge in a vacuum. Not only is it the product of lengthy, multinational negotiations, it also sits in a legal ecosystem that has been thinking about privacy for some time.[76] However, only a few corners of that ecosystem speak to the law of design, and none of that

68. *Id.*
69. *Id.* at art. 5.
70. *Id.* at 29.
71. *Id.* at art. 47.
72. *Id.* at 1.
73. *Id.* at 2.
74. *Id.*
75. *Id.* at 31.
76. Legal interpretations are also made by real people affected by biases, social influences, and institutional pressures. This is one of the core insights of the field of the sociology of law—namely, that law is a social system made up of people and behaviors and a social institution that has an impact on social life. *See, e.g.*, JOHN R. SUTTON, LAW/SOCIETY: ORIGINS, INTERACTIONS, AND CHANGE 8–20 (Sanford Robinson & Cindy Bear eds., Pine Forge Press 2001).

history helps make Article 25 a faithful reflection of the privacy by design literature.

The European Union's Data Privacy Directive (Directive), which the GDPR replaced, referenced privacy by design in its recitals. These provisions, however, were more focused on security than anything else. For example, Recital 46 of the Directive called for "appropriate technical and organizational measures" for safeguarding data "at the time of the design of the processing system and at the time of the processing itself" in order "to maintain security and thereby to prevent any unauthorized processing."[77] The recital repeated this security focus when it noted that companies should consider the state of existing technology and the costs of implementation before deploying tools to "ensure an appropriate level of security."[78] And Article 4(1) of the European Union's Directive on Privacy and Electronic Communications required telecommunication platforms to "take appropriate technical and organisational measures to safeguard [the] security of [their] services," thus continuing the Directive's laser-like focus on security.[79]

Thinking about security from the ground up is an important element of privacy by design. But privacy and security are different—the latter is a component, and not a sufficient one, of the former. Security is about protecting a database of information from outside access and attack, whereas privacy and data protection are far more about the guardrails for internal use of data.[80] Privacy is a social practice made up of norms, rules, and behaviors.[81] It reflects our ongoing negotiations about our place in society, about whether others should have access to us, and about how we manage that access.[82] Therefore, privacy can be an "antisocial retreat" and "essential for personality development, intimacy, group relationships, and freedom from judgment and discrimination."[83] Cyber security is about preventing, assessing, and addressing attacks on data safety and integrity

77. *See* Directive 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, 35 [hereinafter EU Privacy Directive].

78. *Id.*

79. *See* Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, 2002 O.J. (L 201) 37, art. 4(1) [hereinafter EU Privacy & Electronic Communications Directive].

80. *What is the Difference Between Data Security and Data Privacy*, MANAGED SOLUTION (Jan. 23, 2020), https://www.managedsolution.com/data-security-vs-data-privacy-why-it-matters/ [https://perma.cc/98QA-ZV7V].

81. Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CALIF. L. REV. 957, 957 (1989) (arguing that privacy is important specifically because we live in a society where other people are around).

82. HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 157 (Stanford Univ. Press 2010) (offering a theory of "contextual integrity" in which contextual norms shape privacy protection); DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 9 (Harvard Univ. Press 2008) (arguing that privacy should be understood as a family of interrelated problems).

83. ANITA L. ALLEN, UNEASY ACCESS: PRIVACY FOR WOMEN IN A FREE SOCIETY 50 (Rowman & Littlefield 1988) (arguing that privacy should be understood as modes of

once collected and stored.[84] President Barack Obama's Cyberspace Policy Review, for example, defined cyber security as:

> [S]trategy . . . regarding the security of and operations in cyberspace, and encompass[ing] the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities . . . as they relate to the security and stability of the global information and communications infrastructure.[85]

Legal scholars have offered similar definitions, focused on "criminality" and "espionage."[86] Adequate privacy is impossible without adequate security, but designing for security addresses only one part of the playing field.

In an analysis of Article 25, Lee Bygrave pointed to a few design law antecedents from the Directive that go beyond security.[87] For example, Recital 30 of the Directive recommended that communications networks "be designed to limit the amount of personal data necessary to a strict minimum," reflecting the importance of data minimization.[88] And Article 14(3) required that equipment be "constructed in a way that is compatible with the right of users to protect and control the use of their personal data,"[89] reflecting the right of access and principles of control. Therefore, although some of Article 25 may be based on language from the Directive, it is not clear how that helps. Vague and mostly non-binding language in one statute inadequately informs vague language in another. Security by design is embodied in Articles 24 and 32 of the GDPR.[90] Therefore, even considering the design-related rhetoric of the Directive, Article 25 remains repetitious of other provisions.

D. Precedent

The next step, then, is to consider any case law that speaks to design requirements. Granted, the Court of Justice is not bound by *stare decisis*.[91] But the Court rarely departs from its previous decisions in practice.[92] The

---

inaccessibility and noninterference, underscoring privacy's value to enhance personhood, intimacy, and relationships, and women's equal participation in society).

84. Margaret Rouse, *What is Cybersecurity? Everything You Need to Know*, TechTarget (Apr. 2020), https://searchsecurity.techtarget.com/definition/cybersecurity [https://perma.cc/QM5G-Z8QR].

85. U.S. Dep't. of Homeland Sec., Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure iii (2010).

86. Gus P. Coldebella & Brian M. White, *Foundational Questions Regarding the Federal Role in Cybersecurity*, 4 J. Nat'l Security L. & Pol'y 233, 236 (2010).

87. *See generally* Lee A. Bygrave, *Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements*, 4 Oslo L. Rev. 105 (2017).

88. *See* EU Privacy & Electronic Communications Directive, *supra* note 79, at 34.

89. *See id.* at art. 14(3). *See also* Bygrave, *supra* note 87, at 108.

90. *See* GDPR, *supra* note 1, arts. 24, 32.

91. *See* Joined Cases C-267/91 & C-268/91, Criminal Proceedings Against Keck and Mithouard, 1993 E.C.R. I-6126, ¶¶ 14, 16 (stating that "the Court considers it necessary to re-examine and clarify its case-law on this matter" and delivering a decision "contrary to what has previously been decided.").

92. *See* Arnull, *supra* note 34, at 627–28. There are, of course, exceptions to this usual practice. *See, e.g.*, Case C-368/95, Familiapress v. Bauer Verlag, 1997 E.C.R. I-

only major European case that could inform interpretations of Article 25, however, is a 2008 case from the European Court of Human Rights (ECHR), *I v. Finland*.[93] In *Finland*, an HIV-positive woman alleged that the hospital that processed her medical information used a records platform that was designed with inadequate privacy protections.[94] In particular, the system had no access logs.[95] That design flaw made it impossible to determine if anyone had accessed her information without authorization.[96] Finnish law allowed the victim to sue for damages for unauthorized access, but that was not enough for the ECHR.[97] Interpreting Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (the Convention), which guarantees citizens a right to privacy,[98] the ECHR held that Finland had to go further and guarantee privacy by design.[99] The court concluded that "[w]hat is required . . . is practical and effective protection to exclude any possibility of unauthorised access occurring in the first place. Such protection was not given here."[100] In other words, the State had a legal obligation to ensure that the medical records platform its hospitals used was designed from the ground up to prevent, or at least document, unauthorized access to personal information. After all, as the court noted, "had the hospital provided a greater control over access to health records by restricting access to health professionals directly involved in the applicant's treatment . . . the applicant would have been placed in a less disadvantaged position before the domestic courts."[101] That is the role of privacy by design.

Finland is significant. It is an example of a court translating a concept like privacy by design into a real obligation imposed on real people to protect privacy. In so doing, it provided an example of the kind of technical measures—logs, access restrictions, and automatic records—that should be designed into technologies to adequately protect Europeans' right to privacy. But the case's capacity to define the meaning of Article 25 may be limited. *Finland* concerned access to medical information, in general, and

---

3689 (departing from the rule in Cases 60 and 61/84, Cinetheque v. Federation Nationale des Cinemas Francais, 1985 E.C.R. 2605, and holding that national legislation, which was justified under the mandatory requirements doctrine, was not necessary to show that fundamental rights were being respected). *See also* Case C-10/89, CNL-Sucal NV v. HAG GF AG, 1990 E.C.R. I-3711 (expressly overruling the doctrine of common origin, which limited when a trademark owner in one country could restrain imports of products bearing the mark in another country).

93. I v. Finland, App. No. 20511/03 (2008), https://hudoc.echr.coe.int/eng#{%22appno%22:[%2220511/03%22],%22itemid%22:[%22001-87510%22]} [https://perma.cc/MK6H-4HYX].

94. *Id.*

95. *Id.* ¶ 44.

96. *Id.*

97. *Id.* ¶¶ 44–47.

98. *See* Convention for the Protection of Human Rights and Fundamental Freedoms art. VIII, Nov. 4, 1950, E.T.S. No. 5., 213 U.N.T.S. 222 [hereinafter Convention].

99. *See Finland*, *supra* note 93, ¶ 47.

100. *Id.*

101. *Id.* ¶ 44.

a person's HIV status, in particular.[102] These categories of information are considered uniquely private, both in European and American law.[103] Indeed, the ECHR made much of the sensitivity of medical data, calling its protection "fundamental," "vital," and "crucial" all in one paragraph.[104] And a person's HIV status may demand even more protection given the continued stigma faced by HIV-positive individuals.[105] *Finland* was also decided by the ECHR, not the Court of Justice.[106] And technically, the Convention is not formally part of the European legal system.[107] The two courts represent distinct, but overlapping, legal systems. As such, translation from one to the other is possible, though far from certain.

E. Context

Context-based interpretations of EU legislation are common at the Court of Justice. Instead of relying on plain language, recitals, or precedent, contextual analysis looks at other clauses in the statute to clarify confusing provisions.[108] Like U.S. courts, the CJEU follows the principles of *effet utile*, which assumes that each provision of a law has its own unique meaning, thus avoiding redundancy.[109] The court also reads ambiguous provisions to be consistent with the general statute of which they are a

102. *See generally id.*

103. *See, e.g.*, Mark A. Rothstein, *Discrimination Based on Genetic Information*, 33 JURIMETRICS J. 13, 13–18 (1992) (arguing that genetic information deserves special privacy protection); Scott Skinner-Thompson, *Outing Privacy*, 110 NW. U. L. REV. 159, 206 n.251 (2015) (collecting cases suggesting that HIV and other medical information is considered uniquely private); Richard C. Turkington, *Legacy of the Warren and Brandeis Article: The Emerging Unencumbered Constitutional Right to Informational Privacy*, 10 N. ILL. U. L. REV. 479, 511 (1990) (noting that medical information has "special force" because of "both the intrinsic and consequential features of such information"). *See also* Doe v. Barrington, 729 F. Supp. 376, 384 (D.N.J. 1990). *See generally* Doe v. Am. Red Cross Blood Serv., 125 F.R.D. 646 (D.S.C. 1989); Woods v. White, 689 F. Supp. 874 (W.D. Wis. 1988).

104. *Finland*, *supra* note 93, ¶ 38.

105. *See HIV/AIDS at 30: A Public Opinion Perspective*, HENRY J. KAISER FAM. FOUND. 6–9 (2011), https://www.kff.org/wp-content/uploads/2013/07/8186-hiv-survey-report_final.pdf [https://perma.cc/Z5ES-2EX3] (describing the continued stigma towards those living with HIV).

106. *See generally Finland*, *supra* note 93.

107. The Convention was drafted under the auspices of the Council of Europe, the Strasbourg, France-based organization of forty-seven member states established to protect human rights in Europe after World War II. The European Union is the economic and political union of Europe comprised of twenty-eight members. Although all twenty-eight EU members are members of the Council of Europe and EU legal institutions cite Strasbourg cases, the two regimes are technically distinct. *See* Joshua Kleinfeld, *Two Cultures of Punishment*, 68 STAN. L. REV. 933, 952 n.66 (2016) (discussing the differences between the Council of Europe and the EU).

108. *See* LASOK ET AL., *supra* note 34, at 387; Lenaerts & Gutiérrez-Fons, *supra* note 3, at 20. *See also* Case C-66/99, D. Wandel GmbH v. Hauptzollamt Bremen, 2001 E.C.R. I-873, ¶¶ 47-49 (reading several provisions of the Customs Code together to understand the scope and meaning of the clause at issue).

109. *See* SACHA PRECHAL, DIRECTIVES IN EC LAW 259 (Oxford Univ. Press 2d ed. 2005); Lenaerts & Gutiérrez-Fons, *supra* note 3, at 17–20. *See also* LINDA D. JELLUM, MASTERING STATUTORY INTERPRETATION 132 (Cal. Acad. Press 2d ed. 2013) (noting that this is called the "rule against surplusage" in American law).

part.[110] Applying this approach to the GDPR, however, makes Article 25(1) indistinct from the rest of the statute yet again.

Section 2 of Article 25 calls for limitations on access and data minimization "by default,"[111] meaning that only personal data which is necessary for the specific purpose for which it is gathered can be used, and companies must place limits on who can access personal information.[112] At its core, Article 25(1) requires data controllers to "implement appropriate technical and organisational measures . . . which are designed to implement data-protection principles . . . in an effective manner and to integrate the necessary safeguards into the processing [of data] in order to meet the requirements of this Regulation."[113] Both those "data protection principles" and the requirements of Section 2 are outlined in Article 5 of the GDPR,[114] listed in Recital 78,[115] and required by other provisions in the GDPR.

Article 6(1)(a) states that data processing is lawful only when users consent and Article 7 lays out the conditions for lawful consent.[116] Article 8 focuses on the consent necessary to process a child's data.[117] Article 9(2)(a) allows a data subject to consent to the processing of data that reveals racial or ethnic origin or other highly intimate data.[118] Articles 13(2)(c) and 14(2)(d) guarantee the right to withdraw consent in certain circumstances.[119] Article 22 states one of the ways to permit automated decision-making is with "explicit consent."[120]

Data minimization is embodied in Article 47, which requires companies to adopt binding corporate rules on all of the guarantees in Article 5, and in Article 89, which covers data retention for historical and research purposes.[121] Article 15, and to a lesser extent Article 46, guarantees the right of access.[122] Article 12(1) focuses on transparency and clear, concise communication with data subjects.[123] Also, Article 5's security principle is embodied in Article 24(2), which requires data collectors to adopt policies that ensure secure processing, and Article 32(1), which mandates that they only work with pseudonymized or encrypted data.[124]

Other than as a reminder to comply with these clauses, Article 25 only acts as a hedge against noncompliance. Article 83(2)(d), for example,

110. *See* JELLUM, *supra* note 109, at 127–30 (this rule is sometimes called *in pari materia*).
111. *See* GDPR, *supra* note 1, at art. 25(2).
112. *Id.*
113. *Id.* at art. 25(1).
114. *Id.* at art. 5.
115. *Id.* at 15.
116. *Id.* at arts. 6(1)(a), 7.
117. *Id.* at art. 8.
118. *Id.* at art. 9(2)(a).
119. *Id.* at arts. 13(2)(c), 14(2)(d).
120. *Id.* at art. 22(2)(c).
121. *Id.* at arts. 47, 89.
122. *Id.* at arts. 15, 46.
123. *Id.* at art. 12(1).
124. *Id.* at arts. 24(2), 32(1)(a).

states that when determining fines for failure to follow the GDPR's rules, any "technical and organisational measures" the company took to comply with Article 25 should be taken into account.[125] Moreover, the Article 34 requirement to inform users of data breaches can be weakened if the controller has "implemented appropriate technical and organisational protection measures."[126] In the context of these other provisions, then, Article 25 lacks an identity or contribution of its own.[127]

F. Teleological Interpretation

With a teleological approach, the CJEU may go outside the statute and construe legislation in light of the general goals of the EU as a whole.[128] And when legislation, like the GDPR, is meant to realize fundamental freedoms, their provisions are interpreted broadly and in a way most conducive to giving effect to those freedoms and to ensuring that any given provision retains its effectiveness.[129] This method may sound strange to U.S. audiences, but the approach is a "function of the dynamic character of the process of [European] integration" and supports the overarching objective of

125. *Id.* at art. 83(2)(d).

126. *Id.* at art. 34(3)(a).

127. Article 29 Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, now called the Data Protection Board (DPB), could be another source of clarity. The DPB is an advisory group consisting of representatives from the various data protection authorities from EU member states. Since 1997, it has issued 240 statements, reports, opinions, and recommendations to help companies comply with European data protection rules. *See generally Opinions and Recommendations*, EUR. COMMISSION, http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm [https://perma.cc/2BCE-WJV5] (last visited May 3, 2018). Some of the group's recommendations touch on design. For example, in 2014, the Working Party noted that companies that "place privacy and data protection at the forefront of product development will be well placed to ensure that their goods and services respect the principles of privacy by design and are equipped with the privacy friendly defaults expected by EU citizens." *Opinion 8/2014 on the Recent Developments on the Internet of Things*, EUR. COMMISSION 1, 3 (Sept. 16, 2014), http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf [https://perma.cc/DHC3-K6VP]. Its advice to companies working in the Internet of Things marketplace was to "apply the principles of Privacy by Design and Privacy by Default." *Id.* at 21. This language is somewhat unhelpful in crafting meaning for Article 25 independent of the rest of the GDPR, especially where the "principles of privacy by design" are embedded elsewhere in the statute. *See id.* at 3.

128. *See* Jens C. Dammann, *The Right to Leave the Eurozone*, 48 TEX. INT'L L.J. 125, 137 (2013); Nial Fennelly, *Legal Interpretation at the European Court of Justice*, 20 FORDHAM INT'L L.J. 656, 664 (1996) (calling the teleological approach the "characteristic element in the [CJEU]'s interpretive method"). *See also, e.g.*, Case 374/87, Orkem v. Comm'n, 1989 E.C.R. 3283, ¶ 28 (stating that "it is appropriate to consider whether and to what extent the general principles of Community law, of which fundamental rights form an integral part and in the light of which all Community legislation must be interpreted" require the right to remain silent); Joined Cases C-322/99 & C-323/99 Finanzamt Burgdorf v. Fischer, 2001 E.C.R. I-4049, ¶ 75 (rejecting an argument because it would run "counter to the objective of equal treatment").

129. *See* Lenaerts & Gutiérrez-Fons, *supra* note 3, at 20. *See, e.g.*, Case C-434/97, Comm'n v. Fr., 2000 E.C.R. I-1129, ¶ 21; Case 187/87 Saarland & Others v. Ministre de l'Industrie & Others, 1988 E.C.R. 5013, ¶ 19.

the EU of creating "an ever closer union among the peoples of Europe."[130]

European legal scholars have identified three modes of teleological interpretation. One mode ensures the *effet utile*, or effectiveness, of the legislation.[131] Under this approach, a court would identify the normative context in which the law was passed and then interpret the provision at issue in a way that helps it achieve those normative goals.[132] The second mode, used when the law at issue is ambiguous, asks the court to imbue the provision with enough meaning to pursue its objectives.[133] This was the interpretive method used in *Bodil Lindqvist*, where the CJEU broadly interpreted "information" in the Directive in light of the Directive's purpose to protect "the right to respect for private life."[134] The third teleological approach focuses on the consequences to the European Union and its citizens if the Court interpreted a provision in a given way.[135] Any (or all) of these methods are applicable to Article 25(1).

Article 6, Section 2 of the EC Treaty commits the European Union to protecting the fundamental rights of all European citizens as guaranteed by the Convention .[136] Article 8 of the Convention guarantees "the right to respect for his private and family life, his home and his correspondence."[137] This certainly justifies the EU's exercise of power to draft and enact the GDPR; to protect the data subject's right to access, transparency, confidentiality, anonymity, and control; and to ensure that the GDPR is adequately and appropriately enforced. That the GDPR effectuates a basic human right guaranteed to all European citizens also counsels in favor of a broad interpretation.

Therefore, teleological reasoning could add meaning to Article 25(1) in light of these greater goals of the European Union. A broad vision of Article 25(1) transforms it into a kind of catch-all provision, scooping up anything omitted from other, more specific sections of the GDPR. After all, Section 1 boils down to requiring companies to take steps simply to "implement data-protection principles."[138] Given the limitations of language and the drafting process, filling gaps could only empower the GDPR. But the provision also focuses on steps companies need to take to "protect the rights of data subjects."[139] Indeed, it is difficult to imagine something not

130. Miguel Poiares Maduro, *Interpreting European Law: Judicial Adjudication in the Context of Constitutional Pluralism*, EUR. J. LEGAL STUD., Winter 2007, at 1, 11 (internal quotations and parentheticals omitted).

131. Lenaerts & Gutiérrez-Fons, *supra* note 3, at 25.

132. *See, e.g.*, Case C-439/08, Vlaamse Federatie van Verenigingen van Brood-en Banketbakkers, Ijsbereiders en Chocoladebewerkers (VEBIC) VZW, 2010 E.C.R. I-12471, ¶ 64.

133. *See* Lenaerts & Gutiérrez-Fons, *supra* note 3, at 13.

134. Case C-101/01, Criminal Proceedings Against Bodil Lindqvist, 2003 E.C.R. I-12971, ¶¶ 50, 74.

135. *See, e.g.*, Case 6/64, Costa v. ENEL, 1964 E.C.R. 587, 594 (considering the consequences to the EU if EU law had not been given primacy over national law).

136. EC Treaty, *supra* note 27, at art. 6(2).

137. Convention, *supra* note 98, at art. 8.

138. GDPR, *supra* note 1, art. 25(1).

139. *Id.*

covered by that umbrella, including technical and organizational steps to restrict data flows, data collection, and a wide variety of invasive data uses. This interpretation would allow Article 25(1) to fill almost every gap left open by the GDPR, and it appears to be the only interpretive method available that could throw a lifeline to Article 25(1).

It is worth noting that I resist the critiques offered by some scholars who claim that teleological reasoning has no boundaries, makes the EU undemocratic, or that interpreting a law in the context of greater normative goals, societal changes, and fundamental human values is a bad idea.[140] After all, other interpretative tools fall short. Textualism is inherently conservative, ossifying, and a convenient pretext for its own form of judicial activism.[141] It is also difficult, if not impossible, in a jurisdiction of multiple languages. Legislative history is muddled, and published recitals are themselves subject to drafters' compromises and linguistic machinations.[142] There will also always be gaps in legislation, and only an empowered court can fill them in any meaningful way. And the post-World War II EU project specifically embraced a multicultural, liberal set of values that Europeans expected to be integrated into the new legal regime.

G. The Risks of Vagueness and a Call to Action

That said, there are some risks. Article 25(1) asks data collectors to take steps to implement data protection principles effectively. A literal interpretation makes this obvious. An analysis based on the GDPR's related recitals also finds Article 25(1) parroting other parts of the GDPR. Neither statutory nor case precedent add any specific substance. And a contextual analysis makes clear that Article 25(1) adds nothing to the rest of the GDPR. Only a teleological interpretation, which is difficult to predict, can empower Article 25(1) to require real, meaningful, technological, and structural changes inside companies that create and leverage data collection tools.

And the CJEU must take up this call to act. Weak design mandates weaken the GDPR. Some have criticized the GDPR as little more than the "FIPPs plus" because it perpetuates a regime based on notice, consent, access, confidentiality, and security.[143] Many of its provisions, which explicitly envision a watered-down version of "collaborative govern-

140. *See generally* PATRICK NEILL, THE EUROPEAN COURT OF JUSTICE: A CASE STUDY IN JUDICIAL ACTIVITISM (1995); Gerard Conway, *Levels of Generality in the Legal Reasoning of the European Court of Justice*, 14 EUR. L.J. 787 (2008); Trevor C. Hartley, *The European Court, Judicial Objectivity and the Constitution of the European Union*, 112 LAW Q. REV. 95 (1996).

141. *See* William N. Eskridge, Jr. & Philip P. Frickey, *Foreword: Law as Equilibrium*, 108 HARV. L. REV. 26, 77 (1994). *See also* Daniel A. Farber, Essay, *Do Theories of Statutory Interpretation Matter? A Case Study*, 94 NW. U. L. REV. 1409, 1412–15 (2000).

142. Farber, *supra* note 141, at 1413–14.

143. *See* Woodrow Hartzog, *The Inadequate, Invaluable Fair Information Practices*, 76 MD. L. REV. 952, 955–56 (2017) (calling the GDPR a "FIPs-based law[ ]" and little more than FIPs plus).

ance,"[144] are being undermined by corporate control over the compliance process.[145] Privacy by design represents a qualitatively different approach—one that could create wholesale change in how technology products and data collection tools are made—that cannot be met with another check box or "I Agree" button. Eroding its effectiveness by making it a vassal of other, more modest GDPR obligations undermines the privacy protective goals of the GDPR as a whole.

Moreover, only an empowered Article 25(1) can serve as a model for regulators in the U.S. The Federal Trade Commission, which has already endorsed privacy by design in principle,[146] would learn little about the principle from looking at Article 25(1) if the clause does nothing more than obligate companies to follow the GDPR's other requirements. Without more robust guidance based on a teleological interpretation of the provision, it may be difficult for the FTC to integrate privacy by design into its consent decrees with companies under its jurisdiction. This may deny data subjects in the U.S. the protections afforded by design standards.

As it is today, Article 25(1) is so vague that it cannot inform corporate behavior.[147] Data controllers cannot know what actions, changes, or new strategies are necessary if Article 25 fails to provide sufficient notice of its requirements.[148] Perhaps more importantly, vague mandates leave extraordinary interpretive latitude to regulated entities on the ground, many of whom would seek to minimize their obligations rather than take on pro-consumer responsibilities. Lauren Edelman has demonstrated this problem in the employment discrimination context, arguing that vague requirements in Title VII of the Civil Rights Act of 1965 opened the door for compliance professionals on the ground to interpret their obligations narrowly and create merely symbolic structures of compliance without actually adhering to substantive legal mandates.[149] Vague requirements, then, allow predatory companies to make minor, superficial changes and claim their obligations fulfilled.[150]

---

144. *See generally* Margot E. Kaminski, *Binary Governance: Lessons from the GDPR's Approach to Algorithmic Accountability*, 92 S. CAL. L. REV. 1529 (2019) (describing the GDPR as a form of "collaborative governance" but without the essential oversight of civil society).

145. *See generally* Ari Ezra Waldman, *Privacy Law's False Promise*, 97 WASH. U. L. REV. 773 (2020) [hereinafter *Privacy Law's False Promise*] (showing how privacy law, including the GDPR, is undergoing a process of "legal endogeneity" by which compliance processes are undermining and recasting the law to limit its regulatory impact).

146. FTC Report, *supra* note 16, at 22.

147. This is akin to the arguments in support of the void for vagueness doctrine. *See, e.g.*, Connally v. Gen. Constr. Co., 269 U.S. 385, 391 (1926) (a law is unconstitutionally vague when people "of common intelligence must necessarily guess at its meaning").

148. The Supreme Court made this same argument in *Kolender v. Lawson*, which overturned a vague loitering statute. *See* Kolender v. Lawson, 461 U.S. 352, 357 (1983).

149. *See generally* LAUREN B. EDELMAN, WORKING LAW: COURTS, CORPORATIONS, AND SYMBOLIC CIVIL RIGHTS (Univ. Chi. Press 2016) (developing the theory of legal endogeneity in the context of Title VII and workplace sex discrimination law).

150. *See, e.g.*, *Privacy Law's False Promise*, *supra* note 145, at 18 (arguing that vague privacy laws give companies leeway to recast adherence to the law as mere compliance with symbolic structures that do little to achieve the law's substantive goals). *See also*

Vague laws can also make enforcement arbitrary. If Article 25 remains vague, governments, regulators, and data privacy authorities can determine what interpretation of the law they want to apply based on their prejudices or politics. That undermines the rule of law. Former U.S. Supreme Court Justice Sandra Day O'Connor made this point in a decision striking down a criminal vagrancy and loitering law as unconstitutionally vague: vague statutes permit "a standardless sweep [that] allow policemen, prosecutors, and juries to pursue their personal predilections."[151] It is not difficult to imagine a scenario where a vigorous pro-privacy enforcer in France takes an aggressive view of the design law embedded in the GDPR but a pro-business political appointee at the FTC adopts the most lax interpretation of privacy by design.[152] This eventuality could weaken the reach and dramatically undermine the power of privacy's design law, thus highlighting the need for a clear, doctrinal, teleological guide to interpret Article 25(1)'s practical requirements.

Conclusion

This Article has shown that through most methods of interpretation, Article 25(1) of the GDPR does not reflect privacy by design as traditionally understood. Instead, the provision is a reminder to data collectors to comply with *other* parts of the GDPR, thus transforming the clause into a catch-all provision with little identity of its own. Privacy by design can be so much more, and only a robust teleological interpretation can rescue Article 25(1) from its purgatory. Considering the ways in which the technological architecture of a platform can challenge our privacy, organizing a company to appreciate and value privacy from the executive offices down to the engineers on the ground, coding privacy-protective limitations into the DNA of a product or system, and stepping away from products that cannot be designed to protect privacy, could help realize the goals of both the GDPR and the European Union as a whole. Instead, the GDPR's drafters chose to ignore the power of design and cede a powerful weapon in the fight to maintain our privacy in the digital age. The CJEU must correct that error.

Paul D. Butler, *Poor People Lose: Gideon and the Critique of Rights*, 122 YALE L.J. 2176, 2176 (2013) (making a similar argument with respect to the right to counsel from *Gideon v. Wainwright*, 327 U.S. 335 (1963), suggesting that the grant of counsel to the poor acts as a convenient veneer blocking real substantive reform in the criminal justice system to make it less biased); Josh Constine, *A Flaw-by-Flaw Guide to Facebook's New GDPR Privacy Changes*, TECHCRUNCH (Apr. 18, 2018, 1:00 AM), https://techcrunch.com/2018/04/17/facebook-gdpr-changes/ [https://perma.cc/8FE4-8ZAR] (showing how many of the changes Facebook made to its platform to comply with the GDPR are manipulative, superficial, and not designed with ease of use in mind).

151. *Kolender*, 461 U.S. at 358.

152. *But see* William McGeveran, *Friending the Privacy Regulators*, 58 ARIZ. L. REV. 959, 960–97 (2016) (using case studies of privacy investigations in the United States and Europe to counter the conventional wisdom that European regulators are stricter than their United States counterparts).