University of Colorado Law School
Colorado Law Scholarly Commons

Publications | Colorado Law Faculty Scholarship

2019

The Right to Explanation, Explained

Margot E. Kaminski
University of Colorado Law School

Follow this and additional works at: https://scholar.law.colorado.edu/faculty-articles

 Part of the Computer Law Commons, European Law Commons, Privacy Law Commons, and the Science and Technology Law Commons

Citation Information

Margot E. Kaminski, *The Right to Explanation, Explained*, 34 BERKELEY TECH. L.J. 189 (2019), *available at* https://scholar.law.colorado.edu/faculty-articles/1227.

Copyright Statement

Copyright protected. Use of materials from this collection beyond the exceptions provided for in the Fair Use and Educational Use clauses of the U.S. Copyright Law may violate federal law. Permission to publish or reproduce is required.

This Article is brought to you for free and open access by the Colorado Law Faculty Scholarship at Colorado Law Scholarly Commons. It has been accepted for inclusion in Publications by an authorized administrator of Colorado Law Scholarly Commons. For more information, please contact lauren.seney@colorado.edu.

THE RIGHT TO EXPLANATION, EXPLAINED

Margot E. Kaminski†

ABSTRACT

Many have called for algorithmic accountability: laws governing decision-making by complex algorithms, or artificial intelligence (AI). The EU's General Data Protection Regulation (GDPR) now establishes exactly this. The recent debate over the "right to explanation" (a right to information about individual decisions made by algorithms) has obscured the significant algorithmic accountability regime established by the GDPR. The GDPR's provisions on algorithmic accountability, which include a right to explanation, have the potential to be broader, stronger, and deeper than the requirements of the preceding Data Protection Directive. This Article clarifies, including for a U.S. audience, what the GDPR requires.

DOI: https://doi.org/10.15779/Z38TD9N83H
© 2019 Margot E. Kaminski.

† Associate Professor of Law, University of Colorado Law School. Faculty Director of Privacy at Silicon Flatirons. Affiliated Fellow, Information Society Project at Yale Law School. Thanks to Andrea Bertolini, Kiel Brennan-Marquez, Giovanni Comandé, Matthew Cushing, Natalie Helberger, Max van Drunen, Nico van Eijk, Sarah Eskens, Gianclaudio Malgieri, Nicholson Price, Marijn Sax, and Andrew Selbst, and to the Fulbright-Schuman program, IViR at University of Amsterdam, and Scuola Superiore Sant'Anna for their support. All errors are my own.

TABLE OF CONTENTS

I. INTRODUCTION

Scholars and civil society groups on both sides of the Atlantic have been calling for algorithmic accountability: laws governing decision-making by complex algorithms, or AI.[1] Algorithms can be used to make, or to greatly

1. *See, e.g.*, Mike Ananny & Kate Crawford, *Seeing Without Knowing: Limitations of the Transparency Ideal and Its Application to Algorithmic Accountability*, 20 NEW MEDIA & SOC. 973 (2016) (analyzing the benefits and limitations of transparency in establishing algorithmic accountability); Lee A. Bygrave, *Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling*, 17 COMPUTER L. & SECURITY REP. 17 (2001) (analyzing Art. 15 of the 1995 EC Directive on data protection); Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249 (2008) (examining algorithmic decision-making and calling for transparency, accountability, and accuracy); Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1 (2014) (calling for accountability for automated predictions); Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, 55 B.C. L. REV. 93 (2014) (charting the privacy harms caused by big data and proposing procedural due process); Deven R. Desai & Joshua A. Kroll, *Trust But Verify: A Guide to Algorithms and the Law*, 31 HARV. J.L. & TECH. 1 (2017) (providing a computer scientist's perspective on algorithmic accountability and calling for specific tailored solutions); Mireille Hildebrandt, *The Dawn of a Critical Transparency Right for the Profiling Era*, DIGITAL ENLIGHTENMENT Y.B. 41 (2012) (highlighting the potential of the GDPR to protect individuals in the profiling era); Pauline T. Kim, *Auditing Algorithms for Discrimination*, 166 U. PA. L. REV. ONLINE 189 (2017) (proposing a toolkit to ensure algorithmic accountability); Joshua A. Kroll et al., *Accountable Algorithms*, 165 U. PA. L. REV. 633 (2017) (calling for collaboration on algorithmic accountability across computer science, law, and policy); W. Nicholson Price II, *Regulating Black-Box Medicine*, 116 MICH. L. REV. 421 (2017) (proposing that black-box medical algorithms should be governed through collaborative governance); Neil M. Richards & Jonathan H. King, *Big Data Ethics*, 49 WAKE FOREST L. REV. 393 (2014) (calling for ethical standards to be applied to mass data collection

affect, decisions about credit, employment, education, and more.[2] Algorithmic decision-making can be opaque, complex, and subject to error, bias, discrimination, in addition to implicating dignitary concerns.[3] The literature in

and use); Paul Schwartz, *Data Processing and Government Administration: The Failure of the American Legal Response to the Compute*r, 43 HASTINGS L.J. 1321 (1992) (developing an approach to govern the use of computers and personal data); Daniel J. Steinbock, *Data Matching, Data Mining, and Due Process*, 40 GA. L. REV. 1, 23 (2005) (addressing the use of data matching and mining to identify persons against whom an official action is taken); Andrew Tutt, *An FDA for Algorithms*, 69 ADMIN. L. REV. 83 (2017) (calling for a federal agency to govern algorithms); Tal Z. Zarsky, *Transparent Predictions*, 2013 U. ILL. L. REV. 1503 (2013) (creating a framework for understanding transparency as a regulatory concept in algorithmic accountability); Michal S. Gal, *Algorithms as Illegal Agreements*, 34 BERKELEY TECH. L.J. 67 (2019) (examining potential legal solutions to concerns raised by algorithmic-facilitated coordination); Bryan Casey, Ashkon Farhangi & Roland Vogl, *Rethinking Explanable Machines: the GDPR's "Right to Explanation" Debate and the Rise of Algorithmic Audits in Enterprise*, 34 BERKELEY TECH. L.J. 145 (2019) (discussing machine explainability in the context of the European GDPR's "right to explanation").

2. *See, e.g.*, Citron & Pasquale, *supra* note 1, at 4.

3. *See generally* Margot E. Kaminski, *Binary Governance*, 92 S. CAL. L. REV. (forthcoming Sept. 2019) (identifying three categories of concerns behind calls for regulating algorithmic decision-making: dignitary, justificatory, and instrumental); *see also* Andrew D. Selbst & Solon Barocas, *The Intuitive Appeal of Explainable Machines*, 87 FORDHAM L. REV. 1085, 1118–26 (2018) (discussing the rationales behind calls for explanations of algorithmic decision-making) [hereinafter Selbst & Barocas, *Intuitive Appeal*]. On error, see Citron & Pasquale, *supra* note 1, at 8 ("Scoring systems and the arbitrary and inaccurate outcomes they produce must be subject to expert review."); Crawford & Schultz, *supra* note 1, at 104 ("This aggregation of various agencies' data allows law enforcement to predict or flag individuals as suspicious or worthy of investigation, search, or detention based on the agency's outlined criteria . . . . [T]his method may sometimes lead to erroneous results."); Zarsky, *supra* note 1, at 1506 (noting that "the growing use of predictive practices . . . could be tainted with errors and overinvasive"). On bias and discrimination, see Solon Barocas & Andrew Selbst, *Big Data's Disparate Impact*, 104 CALIF. L. REV. 671, 674 (2016) ("Approached without care, data mining can reproduce existing patterns of discrimination, inherit the prejudice of prior decision makers, or simply reflect the widespread biases that persist in society."); Citron, *supra* note 1, at 1262 (noting that "[t]he biases of individual programmers can have a larger, accumulating effect"); Citron & Pasquale, *supra* note 1, at 13 ("Far from eliminating existing discriminatory practices, credit-scoring algorithms instead grant them an imprimatur, systematizing them in hidden ways."). On dignity, see Bygrave, *supra* note 1, at 18; Isak Mendoza & Lee A. Bygrave, *The Right Not to Be Subject to Automated Decisions Based on Profiling*, *in* EU INTERNET LAW: REGULATION AND ENFORCEMENT 77, 84 (Tatiani Synodinou et al. eds., Springer, 2017) (noting "a concern to uphold human dignity by ensuring that humans (and not their 'data shadows') maintain the primary role in 'constituting' themselves"); Zarsky, *supra* note 1, at 1548; *see also* Meg Leta Jones, *The Right to A Human in the Loop: Political Constructions of Computer Automation and Personhood*, 42 SOC. STUD. SCI. 216 (2017) (exploring the role of dignity in data protection law addressing automated decision-making).

the United States has been largely speculative, operating in a policy vacuum.[4] This is resolutely not, however, the case in the European Union.

On May 25, 2018, the General Data Protection Regulation (GDPR) went into effect in the EU.[5] The GDPR contains a significant set of rules on algorithmic accountability, imposing transparency, process, and oversight on the use of computer algorithms to make significant decisions about human beings.[6] The GDPR may prove to be an example, both good and bad, of a robust algorithmic accountability regime in practice.[7] However, to a U.S. audience, the recent vigorous debate around whether there is a "right to explanation" in the GDPR may inspire confusion.[8] Arguments over the

4. Senator Wyden has, for example, proposed algorithmic accountability as part of his proposed federal privacy legislation. More recently, Senator Wyden and Senator Booker along with Representative Clarke proposed the Algorithmic Accountability Act of 2019. Federal law governing the private sector's use of algorithmic decision-making does not, however, currently exist. *See* S. 2188, 115th Cong. (2018), at 2, 6, 32; *see also* S. _ 116th Cong. (2019) (Algorithmic Accountability Act of 2019).

5. *GDPR FAQs*, EU GDPR.ORG, https://eugdpr.org/the-regulation/gdpr-faqs/ [https://perma.cc/FV79-VBRU] (last visited Mar. 13, 2019).

6. Regulation (EU) 2016/679, of the European Parliament and 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 (General Data Protection Regulation), 2016 O.J. (L 119) 1 at arts. 22, 13, 14, 15 [hereinafter GDPR].

7. *Compare, e.g.*, Tal Z. Zarsky, *Incompatible: The GDPR in the Age of Big Data*, 47 SETON HALL L. REV. 995, 1014–15 (2017), *with* Hildebrandt, *supra* note 1.

8. *See* Maja Brkan, *Do Algorithms Rule the World? Algorithmic Decision-Making in the Framework of the GDPR and Beyond*, INT'L J.L. & INFO. TECH. 1, 13–20 (2019); Casey et al., *supra* note 1; Lilian Edwards & Michael Veale, *Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking for*, 16 DUKE L. & TECH. REV. 17, 44 (2017) [hereinafter Edwards & Veale, *Slave to the Algorithm*]

> In 2016, to the surprise of some EU data protection lawyers, and to considerable global attention, Goodman and Flaxman asserted in a short paper that the GDPR contained a "right to an explanation" of algorithmic decision making. As Wachter et al. have comprehensively pointed out, the truth is not quite that simple.

Lilian Edwards & Michael Veale, *Enslaving the Algorithm: From a "Right to an Explanation" to a "Right to Better Decisions"?*, 16 IEEE SECURITY & PRIVACY 46 (2018); Bryce Goodman & Seth Flaxman, *European Union Regulations on Algorithmic Decision-Making and "a Right to Explanation"*, 38 AI MAG. 50, 55–56 (2017); Gianclaudio Malgieri & Giovanni Comandé, *Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation*, 7 INT'L DATA PRIVACY L. 243, 246 (2017); Mendoza & Bygrave, *supra* note 3, at 16; Antoni Roig, *Safeguards for the Right Not to Be Subject to a Decision Based Solely on Automated Processing (Article 22 GDPR)*, 8 EURO. J. L. & TECH. 1 (2017); Selbst & Barocas, *Intuitive Appeal*, *supra* note 3, at 1106; Andrew D. Selbst & Julia Powles, *Meaningful Information and the Right to Explanation*, 7 INT'L DATA PRIVACY L. 233, 235 (2017); Sandra Wachter, Brent Mittelstadt & Luciano Floridi, *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*, 7 INT'L DATA PRIVACY L. 76 (2017) [hereinafter Wachter et al., *Why a Right to Explanation of Automated Decision-Making Does not Exist*]; Sandra Wachter, Brent Mittelstadt & Chris Russell,

purported right to explanation obscure the true substance and depth of the GDPR's algorithmic accountability regime.

This Article clarifies, including for a U.S. audience, what is and is not required by the GDPR. It contributes to the existing conversation over algorithmic accountability in the GDPR by addressing the authoritative guidelines on automated decision-making.[9] Contrary to several scholars, I understand the GDPR to create a broader, stronger, and deeper algorithmic accountability regime than what existed under the EU's Data Protection Directive (DPD).[10] The debate over the right to explanation threatens to obscure this significant development.

Part II of this Article begins by explaining for a U.S. audience the status of the various interpretative documents that accompany the GDPR. Part III identifies the provisions of the GDPR that apply to algorithmic accountability, and points to textual ambiguities that gave rise to disagreements over the right to explanation. Part IV uses the interpretative documents introduced in Part II, including recent authoritative guidelines, to show how many of the questions left open in the GDPR's text have been subsequently narrowed or resolved. Part V turns to the right to explanation and other transparency mechanisms. Throughout, this Article focuses on the GDPR's requirements for private companies rather than for governments.

II. GDPR BASICS

First, a U.S. audience needs to understand the legal materials at play. The GDPR consists of both text (Articles) and an extensive explanatory preamble. The preambular provisions, known as Recitals, do not have the direct force of law in the EU.[11] A Recital is supposed to "cast light on the interpretation to be

Counterfactual Explanations without Opening the Black Box: Automated Decisions and the GDPR, 31 HARV. J. L. & TECH. 841 (2018) [hereinafter Wachter et al., *Counterfactual*].

9. ARTICLE 29 DATA PROTECTION WORKING PARTY, GUIDELINES ON AUTOMATED INDIVIDUAL DECISION-MAKING AND PROFILING FOR THE PURPOSES OF REGULATION 2016/679, 17/EN. WP 251rev.01 (Feb. 6, 2018) [hereinafter GUIDELINES ON AUTOMATED INDIVIDUAL DECISION-MAKING]. Three pieces address the earlier draft version of these guidelines. Casey et. al, *supra* note 1, at 171; *see generally* Michael Veale & Lilian Edwards, *Clarity, surprises, and further questions in the Article 29 Working Party draft guidance on automated decision-making and profiling*, 2 COMPUT. L. & SECURITY REV. 398 (NEEDS PARA); Wachter et. al, *Counterfactual*, *supra* note 8.

10. *See* Edwards & Veale, *Slave to the Algorithm*, *supra* note 8, at 20–21; Wachter et al., *Why a Right to Explanation of Automated Decision-Making Does Not Exist*, *supra* note 8, at 78; Wachter et. al, *Counterfactual*, *supra* note 8, at 861–71.

11. Wachter et al., *Why a Right to Explanation of Automated Decision-Making Does not Exist*, *supra* note 8, at 80.

given to a legal rule [but] it cannot in itself constitute such a rule."[12] This gives Recitals a liminal legal status—they are not binding law, but they are often cited as authoritative interpretations where the GDPR is vague.[13]

While Recitals can clarify how the GDPR's standards should be applied, they often contain language that goes well beyond what is in the GDPR itself, reflecting the result of political compromise during negotiations.[14] Recitals cannot create new legal requirements, but the line between valid interpretation and invalid creation of new law can be hard to draw.

Discussions of the GDPR also frequently cite interpretative guidelines issued by a group previously known as the Article 29 Working Party and now called the European Data Protection Board.[15] The Working Party/Data Protection Board is made up of Data Protection Authorities (the regulators tasked with enforcing the GDPR) from around the EU who come to a consensus over the interpretation of data protection provisions. As Data Protection Authorities in EU Member States enforce the GDPR on the ground, they refer to the guidelines issued by the Working Party/Data Protection Board.

Article 29 Working Party guidelines, again, do not have the direct force of law. They are, nonetheless, strongly indicative of how enforcers will interpret the law. Now that the GDPR is in effect, these guidelines have additional, though indirect, teeth. The European Data Protection Board under the GDPR has additional supervisory and harmonizing capabilities over Member State Data Protection Authorities.[16] A local Data Protection Authority, in other words, is now even more likely to adhere to the guidelines than under the Directive.

U.S. audiences thus need to understand that while only the text of the GDPR is technically binding law, both Recitals and Working Party/Data Protection Board guidelines play a significant role, in practice, in guiding how

12. Case 215/88 Casa Fleischhandels [1989] European Court of Justice ECR 2789 [31], https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A61988CJ0215 [https://perma.cc/C8RK-45FP].

13. *See, e.g.*, Brkan, *supra* note 8, at 16 ("Dismissing the possibility of the existence of the right to explanation altogether because recitals are not legally binding is too formalistic.").

14. Edwards & Veale, *Slave to the Algorithm*, *supra* note 8, at 50 ("In the GDPR however, as a matter of political expediency, many issues too controversial for agreement in the main text have been kicked into the long grass of the recitals, throwing up problems of just how binding they are.").

15. GDPR, *supra* note 6, at art. 68.

16. *Id.* at art. 70; *see* Amber Hawk, *The Recitals Are Essential to Your Understanding the General Data Protection Regulation*, HAWK TALK (Jan. 28, 2016), http://amberhawk.typepad.com/amberhawk/2016/01/the-recitals-are-essential-to-your-understanding-the-general-data-protection-regulation.html [https://perma.cc/7S5B-AH8E].

companies will behave. A company, concerned about the GDPR's significant penalties (famously up to 4% of worldwide revenue) backed by an increasingly rights-protective European Court of Justice, is likely to follow both the Recitals and Working Party guidance because they are indicative of what the GDPR's enforcers are likely to do.[17] Although these texts are not technically binding, they strongly indicate how enforcers and eventually courts will likely interpret the text.

In another Article, I argue at length that this is precisely how the GDPR is intended to work.[18] The GDPR is, in large part, a collaborative governance regime.[19] The text is full of broad standards, to be given specific substance over time through ongoing dialogues between regulators and companies, backed eventually by courts. Both the Recitals and the Working Party guidelines, along with numerous mechanisms ranging from a formal process for establishing codes of conduct to less formal impact assessment requirements, are part of this collaborative approach.[20]

Thus, when scholars argue that what is in the Recitals is not the law,[21] they are not only insisting on a technicality—distinguishing between harder and softer legal instruments—they are also disregarding the fundamentally collaborative, evolving nature of the GDPR, and removing important sources of clarity for companies as the law develops.

17. GDPR, *supra* note 6, at art. 84. For indicators of the Court's increasing interest in data protection, see, for example, Joint Cases C-293/12 & C-594/12, Digital Rights Ireland Ltd. v. Minister for Commc'ns, ECLI:EU:C:2014:238 (2014) (finding data retention requirements to violate the fundamental right to data protection); Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (AEPD) (2014) (finding that Google as a search engine is a data controller and thus is responsible for affording individuals the data protection right to erasure ("right to be forgotten") from search engine indexing). While the ECtHR is not responsible for GDPR interpretation, it also forms a backstop to surveillance-related law in the EU. *See* Roman Zakharov v. Russia, 2015-VIII Eur. Ct. H.R. 205 (finding Russian metadata surveillance in violation of fundamental rights).

18. *See* Kaminski, *Binary Governance*, *supra* note 3.

19. For discussions of collaborative governance (also known as "new governance"), see, e.g., Jody Freeman, *Collaborative Governance in the Administrative State*, 45 UCLA L. REV. 1 (1997); Orly Lobel, *The Renew Deal: The Fall of Regulation and the Rise of Governance in Contemporary Legal Thought*, 89 MINN. L. REV. 342 (2004).

20. Kaminski, *Binary Governance*, *supra* note 3, at 21–22.

21. *See* Wachter et al., *Why a Right to Explanation of Automated Decision-Making Does Not Exist*, *supra* note 8, at 80.

III. ALGORITHMIC ACCOUNTABILITY IN THE TEXT OF THE GDPR

This Part introduces the text of the GDPR that applies to algorithmic decision-making. There are four Articles of the GDPR that specifically address algorithmic decision-making. Article 22 of the GDPR addresses "[a]utomated individual decision-making, including profiling."[22] Articles 13, 14, and 15 each contain transparency rights around automated decision-making and profiling.[23] More general GDPR provisions, such as the right to object, the right to rectification (correction), data protection by design and by default, and the requirement of data protection impact assessments, likely apply to most or even all algorithmic decision-making.[24] For the sake of brevity and clarity, this Part discusses only the text of Articles 22, 13, 14, and 15, which specifically reference automated decision-making.[25] As others have pointed out, however, the more generally applicable provisions of the GDPR also play an important role in governing algorithmic decision-making.[26]

A. ARTICLE 22: AUTOMATED INDIVIDUAL DECISION-MAKING

Article 22 states that individuals "have the right not to be subject to a decision based solely on automated processing."[27] Scholars have pointed out, based on the historical treatment of similar text in the Data Protection Directive (DPD), the predecessor to the GDPR, that this could be interpreted as either a right to object to such decisions or a general prohibition on significant algorithmic decision-making.[28] Interpreting Article 22 as establishing a right to object would make the right narrower. In practice, it would allow companies to regularly use algorithms in significant decision-making, adjusting their behavior only if individuals invoke their rights.

22. GDPR, *supra* note 6, at art. 22.

23. *See id.* at arts. 13(2)(f), 14(2)(g), 15(1)(h).

24. *See* Edwards & Veale, *Slave to the Algorithm*, *supra* note 8, at 19 (noting "other parts of the GDPR related (i) to the right to erasure ('right to be forgotten') and the right to data portability; and (ii) to privacy by design, Data Protection Impact Assessments and certification and privacy seals"), 23, 77; Casey et. al, *supra* note 8, at 173–76 (discussing DPIA safeguards); GUIDELINES ON AUTOMATED INDIVIDUAL DECISION-MAKING, *supra* note 9, at 29 (discussing DPIA and data protection officer), 34 (discussing right to object); *see also* GDPR, *supra* note 6, Recital 91 (described as "[n]ecessity of a data protection impact assessment").

25. *See generally* GDPR, *supra* note 6, at arts. 13, 14, 15, 22.

26. *See* Edwards & Veale, *Slave to the Algorithm*, *supra* note 8, at 19.

27. GDPR, *supra* note 6, at art. 22(1).

28. *See, e.g.*, Mendoza & Bygrave, *supra* note 3, at 9 ("[t]his distinction . . . suggests that Art. 22(1) is intended as a prohibition and not a right that the data subject has to exploit" but noting that it can be argued both ways); Wachter et al., *Why a Right to Explanation of Automated Decision-Making Does not Exist*, *supra* note 8, at 94.

Interpreting Article 22 instead as a prohibition on algorithmic decision-making would require all companies using algorithmic decision-making to assess which exception they fall under and to implement safeguards to protect individual rights, or to not deploy algorithmic decision-making at all.

The Article 22 right/prohibition applies only when the decision is "based solely" on algorithmic decision-making, and it applies only when the decision produces "legal effects" or "similarly significant" effects on the individual.[29] What either of these restrictions means is unclear from the GDPR's text alone. One could narrowly interpret "based solely" to mean that any human involvement, even rubber-stamping, takes an algorithmic decision out of Article 22's scope; or one could take a broader reading to cover all algorithmically-based decisions that occur without *meaningful* human involvement.[30] Similarly, one could take a narrow reading of "similarly significant" effects to leave out, for example, behavioral advertising and price discrimination, or one could take a broader reading and include behavioral inferences and their use.[31]

There are three exceptions to the Article 22 right/prohibition. The first is when the automated decision is "necessary for . . . a contract."[32] The second is when a Member State of the European Union has passed a law creating an exception.[33] The third is when an individual has explicitly consented to algorithmic decision-making.[34] Both the contractual exception and the explicit consent exception could be interpreted to be broader or narrower in nature,

29. GDPR, *supra* note 6, at art. 22(1) ("The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.").

30. *See, e.g.*, Mendoza & Bygrave, *supra* note 3, at 11 ("Even if a decision is formally ascribed to a person, it is to be regarded as based solely on automated processing if a person does not actively assess the result of the processing prior to its formalization as a decision."); Wachter et al., *Why a Right to Explanation of Automated Decision-Making Does not Exist*, *supra* note 8, at 88 ("[T]his creates a loophole whereby even nominal involvement of a human in the decision-making process allows for an otherwise automated mechanism to avoid invoking elements of the right of access . . . addressing automated decisions.").

31. *See, e.g.*, Edwards & Veale, *Slave to the Algorithm*, *supra* note 8, at 47–48 (discussing whether advertising constitutes a significant effect), 69 (discussing the GDPR's inconsistent treatment of inferences); Malgieri & Comandé, *supra* note 8, at 265 ("[S]ignificant effects should also include cases of neuromarketing manipulation or price discrimination . . . .").

32. GDPR, *supra* note 6, at art. 22(2)(a) ("[N]ecessary for entering into, or performance of, a contract between the data subject and a data controller.").

33. *Id.* at art. 22(2)(b) ("[A]uthorised by Union or Member State law to which the controller is subject.").

34. *Id.* at art. 22(2)(c) ("[B]ased on the data subject's explicit consent.").

depending for example on how one interprets "necessary for . . . a contract."[35] In the case of sensitive, or "special category," data, even fewer exceptions apply.[36]

Even when an exception to Article 22 applies, a company must implement "suitable measures to safeguard the data subject's rights and freedoms and legitimate interests . . . ."[37] This requirement is the source of the debate over the right to explanation. Suitable safeguards, according to the text, must include "at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision."[38] This explicitly creates a version of algorithmic due process: a right to an opportunity to be heard.[39] These are the only safeguards named in the GDPR's text. The use of the words "at least," however, indicates that these are an open list of minimum requirements, and a company should do more. As discussed in Part IV, both the preamble (Recital) and interpretative guidance have added to this list of both suggested and required safeguards, and both include as a safeguard a right to explanation of an individual decision.

One important note on suitable safeguards: the specific minimum examples above apply with respect to the contractual exception and explicit consent exception, but are not in the text of the Member State law exception.[40] This textual difference leaves room for the possibility that Member States might enact a different set of suitable safeguards.[41] It remains to be seen whether Data Protection Authorities and courts will allow Member States to adopt significantly different protections against algorithmic decision-making.

35. Mendoza & Bygrave, *supra* note 3, at 14–15; Wachter et al., *Why a Right to Explanation of Automated Decision-Making Does not Exist*, *supra* note 8, at 98.

36. GDPR, *supra* note 6, at art. 22(4) ("Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies . . . .").

37. GDPR, *supra* note 6, at arts. 22(2)(b), 22(3).

38. GDPR, *supra* note 6, at art. 22(3).

39. Several U.S. scholars have called for algorithmic due process, mimicking procedural due process rights. *See* Citron & Pasquale, *supra* note 1; *see generally* Crawford & Schultz, *supra* note 1.

40. GDPR, *supra* note 6, at arts. 22(2)(b), 22(3).

41. Wachter et al. argue that this means that the same safeguards do not apply. Wachter et al., *Why a Right to Explanation of Automated Decision-Making Does not Exist*, *supra* note 8, at 93; Brkan, *supra* note 8, at 12 (describing German law); *see* Gianclaudio Malgieri, Automated Decision-Making in the EU Member States; The Right to Explanation and other 'Suitable Safeguards' (Aug. 17, 2018) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3233611 [https://perma.cc/WLC6-X8QC].

B. ARTICLES 13, 14, AND 15: NOTIFICATION AND ACCESS RIGHTS

Outside of Article 22, the GDPR contains a series of individual notification and access rights specific to automated decision-making. Article 13 establishes a series of notification rights/requirements when information is collected directly from individuals.[42] Article 14 establishes a similar set of notification rights/requirements when information about individuals is collected from third parties.[43] Article 15 creates an individual right of access to information held by a company that can be invoked "at reasonable intervals."[44] All three Articles contain an identical provision requiring disclosure of "the *existence* of automated decision-making, including profiling."[45] Additionally, this provision requires disclosure of "*meaningful information about the logic involved*, as well as the significance and the envisaged consequences of such processing for the data subject."[46]

This language has provoked debate, especially over the question of timing.[47] The language in all three Articles is identical, but the temporal context is different. Articles 13 and 14, roughly speaking, require companies to notify individuals when data is obtained,[48] while Article 15 creates access rights at almost any time. Some scholars have argued that because the text of the three Articles is identical, it must refer to the same information, which indicates that "meaningful information about the logic involved" can be only a broad

42. GDPR, *supra* note 6, at art. 13.

43. *Id.* at art. 14.

44. *Id.* at art. 15. *See* GDPR, *supra* note 6, Recital 63 (described as "[r]ight of access").

45. GDPR, *supra* note 6, at arts. 13(2)(f), 14(2)(g), 15(1)(h) (collectively, "meaningful information" provisions) (emphasis added).

46. GDPR, *supra* note 6, at arts. 13(2)(f), 14(2)(g), 15(1)(h).

47. *See, e.g.*, Mendoza & Bygrave, *supra* note 3, at 16 ("[T]he wording of Art. 15 does not *necessarily* exclude the possibility that it embraces a right of ex post explanation of an Art. 22 type decision."); Selbst & Powles, *supra* note 8, at 236; Wachter et al., *Why a Right to Explanation of Automated Decision-Making Does not Exist*, *supra* note 8, at 90 ("As the scope of information data controllers are required to disclose in Article 15 is the same as in Article 13, Article 15 similarly requires only limited information about the functionality of the automated decision-making system.").

48. GDPR, *supra* note 6, at art. 13 (requiring it when data is obtained); *id.* at art. 14(3)(a) (requiring disclosure "within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed"). Article 14 also envisions notification in communication with a data subject where data is used for communication (art. 14(3)(b)) or upon disclosure of data to another third party (art. 14(3)(c)). These both refer to a later notification than upon obtaining data, but it is harder to envision when this might refer to algorithmic decision-making that has already occurred (unless one is communicating the results to an individual or third party, perhaps?).

overview of a decision-making system.[49] Others argue, however, that, read in context, "meaningful information" must mean multiple things.[50] Articles 13 and 14 might require an overview of a system prior to processing, but Article 15's access right could provide deeper disclosure, including insight into a particular decision affecting a particular individual. The text of the GDPR does not clarify this conflict one way or another.

There are exceptions to the GDPR's notification and access requirements.[51] While not included in the text of the GDPR, an accompanying Recital mentions an exception for intellectual property rights—that is, trade secrets and copyright law.[52] Some scholars argue that, in practice, trade secrets, in particular, represent a significant obstacle to meaningful disclosure of algorithms.[53] This has certainly been the case in the United States.[54] Others observe, however, that fundamental rights such as the right to data protection take precedence over trade secrecy.[55]

The text of the GDPR thus creates both transparency and process rights around algorithmic decision-making. The text itself, however, leaves considerable room for interpretation. But both accompanying and subsequent interpretative documents narrow and clarify the GDPR's text, resolving a number of the conflicts discussed above.

---

49. Wachter et al., *Why a Right to Explanation of Automated Decision-Making Does Not Exist*, *supra* note 8, at 82.

50. *See, e.g.*, Malgieri & Comandé, *supra* note 8, at 244; Mendoza & Bygrave, *supra* note 3, at 16; Selbst & Powles, *supra* note 8, at 236.

51. *See* GDPR, *supra* note 6, at arts. 14(5), 15(4).

52. *See* GDPR, *supra* note 6, Recital 63 ("That right should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software."). The copyright argument makes little sense. *See* Brkan, *supra* note 8, at 22.

53. Wachter et al., *Why a Right to Explanation of Automated Decision-Making Does Not Exist*, *supra* note 8, at 85.

54. *See, e.g.*, Jessica M. Eaglin, *Constructing Recidivism*, 67 EMORY L.J. 59, 111 (2017) ("Transparency Measures"); David S. Levine, *The Impact of Trade Secrecy on Public Transparency*, *in* THE LAW AND THEORY OF TRADE SECRECY: A HANDBOOK OF CONTEMPORARY RESEARCH 406 (Rochelle C. Dreyfuss & Katherine J. Strandburg eds., 2010); Rebecca Wexler, *Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System*, 70 STAN. L. REV. 1343, 1349–50 (2018).

55. Brkan, *supra* note 8, at 21–24; Malgieri & Comandé, *supra* note 8, at 262; Selbst & Powles, *supra* note 8, at 242.

IV. ALGORITHMIC ACCOUNTABILITY IN THE GDPR, INTERPRETED

Both the Recitals and recently adopted Working Party guidelines clarify the GDPR's text in important ways. Article 22 and the "meaningful information" provisions are not devoid of substance; they create an algorithmic accountability regime that is broader, stronger, and deeper than what existed in Europe prior to the GDPR.[56] This Part first explains how the GDPR's text has been clarified, with reference to the debates discussed in Part III above.[57] It then explains why the GDPR's version of algorithmic accountability is broader, stronger, and deeper than Article 15 of the DPD.

First, the Working Party guidelines clarify that Article 22 is a prohibition on algorithmic decision-making, not a mere right to object to it.[58] This is significant because it clarifies that companies have a duty *not to use* solely automated decision-making, rather than a mere duty to respond to individuals who object to it. Companies using algorithmic decision-making will, therefore, have to assess which exception they fall under (contract, explicit consent, or Member State law), which will often trigger additional disclosures to individuals as companies attempt to obtain explicit consent or to justify why such decision-making is necessary to a contract.[59]

Second, the guidelines explain that for an automated decision to fall outside of Article 22, human involvement must be meaningful.[60] A company does not escape Article 22 solely by having a human rubber-stamp algorithmic decisions.[61] Human oversight must be "carried out by someone who has the authority and competence to change the decision."[62] That person must additionally have access to information beyond just the algorithm's outputs.[63] The GDPR will thus have the effect of requiring companies to think about

56. *See* GDPR, *supra* note 6, at arts. 13(2)(f), 14(2)(g), 15(1)(h).

57. For another (more pessimistic) take on the guidelines, see Veale & Edwards, *supra* note 9.

58. GUIDELINES ON AUTOMATED INDIVIDUAL DECISION-MAKING, *supra* note 9, at 19.

59. *Id.* at 13 ("Controllers seeking to rely upon consent as a basis for profiling will need to show that data subjects understand exactly what they are consenting to . . . .").

60. *Id.* at 21 ("The controller cannot avoid the Article 22 provisions by fabricating human involvement [, and] must ensure that any oversight of the decision is meaningful, rather than just a token gesture.").

61. *Id.* ("[I]f someone routinely applies automatically generated profiles to individuals without any actual influence on the result, this would still be a decision based solely on automated processing.").

62. *Id.*

63. *See id.* (noting that the controller "should consider all the relevant data" during analysis of the decision).

how they structure their "human in the loop" of algorithmic decision-making to escape Article 22's prohibition or forego its safeguard requirements.[64]

Third, both Recital 71 and the guidelines provide examples of decisions with significant effects. Recital 71 provides examples of credit determinations and e-recruiting practices.[65] The Working Party guidelines explain that "only serious impactful effects" will trigger Article 22.[66] The guidelines provide both a framework for determining what constitutes a significant effect[67] and a list of examples: decisions that affect financial circumstances or access to health services or access to education, or decisions that deny employment or put someone "at a serious disadvantage."[68]

The guidelines additionally, and perhaps surprisingly, explain that some behavioral advertising will be covered.[69] Particularly intrusive advertising targeted at particularly vulnerable data subjects in particularly manipulative ways will trigger Article 22.[70] Differential pricing—showing people different prices based on personal profiles—could also trigger Article 22 if "prohibitively high prices effectively bar someone from certain goods or services."[71] Thus Article 22's algorithmic accountability provisions will reach

64. *See* Citron & Pasquale, *supra* note 1, at 6–7; *see also* Meg Leta Jones, *The Ironies of Automation Law: Tying Policy Knots with Fair Automation Practices Principles*, 18 VAND. J. ENT. & TECH. L. 77 (2015).

65. GDPR, *supra* note 6, Recital 71

> [S]uch as automatic refusal of an online credit application or e-recruiting practices without any human intervention . . . in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her.

66. GUIDELINES ON AUTOMATED INDIVIDUAL DECISION-MAKING, *supra* note 9, at 21. Examples of legal effects in the guidelines largely involve government use of algorithms rather than use by private companies but include the cancellation of a contract. The guidelines list as examples: entitlement to or denial of a social benefit granted by law; and immigration effects. *See* ARTICLE 29 DATA PROTECTION WORKING PARTY, GUIDELINES FOR IDENTIFYING A CONTROLLER OR PROCESSOR'S LEAD SUPERVISORY AUTHORITY, 16/EN, WP 244 (Dec. 13, 2016), at 4 (discussing "substantially affects").

67. GUIDELINES ON AUTOMATED INDIVIDUAL DECISION-MAKING, *supra* note 9, at 21 ("[S]ignificantly affect the circumstances, behaviour or choices of the individuals concerned; have a prolonged or permanent impact on the data subject; or at its most extreme, lead to the exclusion or discrimination of individuals.").

68. *Id.* at 22.

69. *Id.* ("Similarly significant effects could also be triggered by the actions of individuals other than the one to which the automated decision relates.").

70. *Id.*

71. *Id.*

at least some behavioral advertising and some differential pricing tactics. This coverage is broader than some scholars predicted.[72]

Fourth, the Working Party guidelines somewhat close the trade secrets loophole to algorithmic transparency. Several scholars feared that in practice, companies could avoid the GDPR's transparency requirements by citing a need for corporate secrecy.[73] The guidelines explain, however, that while there is "some protection" against having to reveal trade secrets, companies "cannot rely on the protection of their trade secrets as an excuse to deny access or refuse to provide information . . . ."[74] While this does not eliminate the trade secrets exception discussed in Recital 63, it does at least urge data protection authorities to watch for the use of overly broad trade secrets claims.

Fifth, the guidelines clarify that both the contractual exception and the explicit consent exception to Article 22 are relatively narrow.[75] For example, online retailers cannot argue that profiling is necessary for an online purchase, even where profiling is mentioned in the fine print of the contract.[76] Automated decision-making might be necessary where human involvement is impossible due to the sheer quantity of information processed, but then the company must show that there is no other effective and less privacy-intrusive way to accomplish the same goal.[77]

The guidelines similarly constrain the explicit consent exception and turn it into an information-driving tool.[78] They explain that individuals must be provided enough information about the use and consequences of profiling to ensure that any consent "represents an informed choice."[79] The guidelines do not provide additional information about "explicit consent," except to note that while explicit consent is not defined in the GDPR, a "high level of individual control over personal data is . . . deemed appropriate."[80]

---

72. *See* Wachter et al., *Why a Right to Explanation of Automated Decision-Making Does Not Exist*, *supra* note 8, at 92–93, 98; *see, e.g.*, Edwards & Veale, *Slave to the Algorithm*, *supra* note 8, at 47–48 (questioning whether race-targeted advertising constitutes a significant effect on an individual).

73. *See* Wachter et al., *Why a Right to Explanation of Automated Decision-Making Does not Exist*, *supra* note 8, at 85–86; *see also* Edwards & Veale, *Slave to the Algorithm*, *supra* note 8, at 53 ("Article 15(h) has a carve out in the recitals, for the protection of trade secrets and IP.").

74. GUIDELINES ON AUTOMATED INDIVIDUAL DECISION-MAKING, *supra* note 9, at 17.

75. *Id.* at 13 ("[N]ecessity should be interpreted narrowly.").

76. *See id.*

77. *Id.* at 23.

78. *See id.* at 13, 23.

79. *Id.* at 13.

80. *Id.* at 24. *See* ARTICLE 29 DATA PROTECTION WORKING PARTY, GUIDELINES ON CONSENT UNDER REGULATION 2016/679, 17/EN, WP259, (Nov. 28, 2017).

Finally, the guidelines address the central question of what is required as "appropriate safeguards" to protect individuals from automated decision-making when one of the exceptions applies.[81] Scholars have argued that there is no right to an explanation of individual decisions in the GDPR because that right is not specifically enumerated in the GDPR's text.[82] That reasoning is wrong.[83] Recital 71 states that "suitable safeguards . . . should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to *obtain an explanation of the decision reached* after such assessment and to challenge the decision."[84]

The Working Party guidelines directly quote this language, not once but thrice.[85] The guidelines counsel that there is a need for this form of transparency because an individual can challenge a particular decision or express her view only if she actually understands "how it has been made and on what basis."[86] In other words, an individual has a right to explanation of an individual decision because that explanation is necessary for her to invoke the other rights—e.g., to contest a decision, to express her view—that are explicitly enumerated in the text of the GDPR.[87]

Beyond the right to explanation, the guidelines explain that the GDPR establishes a version of individual algorithmic due process by creating an

81. GUIDELINES ON AUTOMATED INDIVIDUAL DECISION-MAKING, *supra* note 9, at 27.

82. Edwards & Veale, *Slave to the Algorithm*, *supra* note 8, at 50 ("Our view is that these certainly seem shaky foundations on which to build a harmoni[z]ed cross-EU right to algorithmic explanation."); Wachter et al., *Why a Right to Explanation of Automated Decision-Making Does Not Exist*, *supra* note 8, at 79.

83. At this point, the bulk of the literature on the right to explanation appears to agree that this reasoning is erroneous. *See* Brkan, *supra* note 8, at 16 ("Dismissing the possibility of the existence of the right to explanation altogether because recitals are not legally binding is too formalistic, in particular in the light of the CoJ's case law which regularly uses recitals as an interpretative aid."); Malgieri & Comandé, *supra* note 8, at 255 ("[T]he right to obtain an explanation of the decision reached after the assessment should always be exercisable."); Mendoza & Bygrave, *supra* note 3, at 16 ("[W]e should not discount the possibility that a right of ex post explanation of automated decisions is implicit in the right 'to contest' a decision pursuant to Art. 22(3)."); Selbst & Powles, *supra* note 8, at 235 ("Recital 71 is not meaningless, and has a clear role in assisting interpretation and co-determining positive law."), 242 ("We believe that the right to explanation should be interpreted functionally, flexibly, and should, at a minimum, enable a data subject to exercise his or her rights under the GDPR and human rights law.").

84. GDPR, *supra* note 6, Recital 71 (emphasis added).

85. GUIDELINES ON AUTOMATED INDIVIDUAL DECISION-MAKING, *supra* note 9, at 19, 27, 35.

86. *Id.* at 27.

87. Both Mendoza & Bygrave and Selbst & Powles suggested precisely this. Mendoza & Bygrave, *supra* note 3, at 16; Selbst & Powles, *supra* note 8, at 242.

opportunity to be heard.[88] The guidelines note that safeguards must include human intervention by a reviewer with "the appropriate authority and capability to change the decision," and who should have access to "all the relevant data."[89] This imposes another form of transparency, albeit internal to a company, as technical information flows to the human called on to intervene in an algorithmic decision. There is little in the guidelines, however, outlining how human intervention and contestation should take place, apart from suggesting that companies provide a link to an appeals process, a timeline for review, and a named contact person for inquiries.[90] This opportunity to be heard thus may prove to be more or less meaningful, in practice, and risks being, as currently described, reduced to the provision of a contact email.

The next interpretative move that the guidelines make might not be intuitive to a U.S. audience expecting a system entirely focused on individual rights. Beyond individual due process, the guidelines interpret "suitable safeguards" to also include systemic accountability measures such as auditing and ethical review boards.[91] These systemic accountability measures have dual meaning: They can be understood as bolstering individual rights by ensuring that somebody impartial is providing oversight in the name of individuals, or as providing necessary accountability over company behavior in a collaborative governance (private/public partnership) regime, as companies come up with and implement systems for preventing error, bias, and discrimination.[92]

In practice, this systemic accountability involves a number of system-wide checks. Scholars have read Recital 71's language to require algorithmic auditing.[93] The Working Party Guidelines support this interpretation, suggesting that safeguards include quality assurance checks, algorithmic auditing, independent third-party auditing, and more.[94] Both Recital 71 and the guidelines also task companies with preventing discrimination in many forms,

88. Several U.S. scholars have called for algorithmic due process that closely mirrors what is in the GDPR. *See, e.g.*, Citron, *supra* note 1; Citron & Pasquale, *supra* note 1; Crawford & Schultz, *supra* note 1.

89. GUIDELINES ON AUTOMATED INDIVIDUAL DECISION-MAKING, *supra* note 9, at 27 (should assess "all the relevant data").

90. *Id.* at 32.

91. *Id.*

92. Kaminski, *Binary Governance*, *supra* note 3, at 34.

93. Malgieri & Comandé, *supra* note 8, at 258–59. GDPR, *supra* note 6, Recital 71 states that companies should adopt "technical and organisational measures appropriate to ensure . . . that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimised."

94. *See* GUIDELINES ON AUTOMATED INDIVIDUAL DECISION-MAKING, *supra* note 9, at 32.

including on the basis of race, ethnic origin, political opinion, religion.[95] The guidelines envision ongoing testing and feedback into an algorithmic decision-making system to prevent errors, inaccuracies, and discrimination on the basis of sensitive ("special category") data.[96]

As for whether Member States are bound to create laws incorporating these same safeguards—that is, whether the GDPR harmonizes safeguards against algorithmic decision-making or leaves space for Member State variations—the guidelines are strongly suggestive but not entirely clear. They state that "Member . . . State law that authorizes [algorithmic decision-making] must also incorporate appropriate safeguarding measures."[97] In the next paragraph, the guidelines state that "[s]uch measures should include as a minimum a way for the data subject to obtain human intervention, express their point of view, and contest the decision."[98] This suggests that the GDPR does harmonize safeguards, even when a Member State creates a new exception to the ban on automated decision-making. But as several scholars point out, Member State laws have already developed variations on Article 22's safeguards.[99]

To return to the larger claim: while the guidelines and Recitals do not eliminate all room for interpretation, they largely clarify the GDPR's algorithmic accountability provisions to make them more, not less, rigorous. These interpretive documents fully close a number of the loopholes suggested by scholars and limit room for others. This causes Article 22 (and accompanying notification and access rights) to be broader, stronger, and deeper than the preceding EU algorithmic accountability regime.[100] The GDPR applies to more activity (is broader), comes with more significant

95. *See id.* at 6, 10, 14 (explaining that even in profiling without automated decision-making, companies should employ "safeguards aimed at ensuring fairness, non-discrimination and accuracy in the profiling process"); *see also* GDPR, *supra* note 6, Recital 71 ("[P]revent, inter alia, discriminatory effects on natural persons on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation, or processing that results in measures having such an effect.").

96. GUIDELINES ON AUTOMATED INDIVIDUAL DECISION-MAKING, *supra* note 9, at 28.

97. *Id.* at 27.

98. *Id.* at 27.

99. *See* Brkan, *supra* note 8, at 12 (describing German law on insurance); *see also* Malgieri, *supra* note 41, at 8-9 (describing variations in Member State laws as to suitable safeguards for algorithmic decision-making).

100. Amy Kapczynski has used similar terms ("broader," "deeper," and "more severe") to describe the ratcheting-up of intellectual property law internationally. Amy Kapczynski, *The Access to Knowledge Mobilization and the New Politics of Intellectual Property*, 117 YALE L.J. 804, 821 (2008).

enforcement (is stronger), and adds significant protections (is deeper), compared to the Data Protection Directive.

Article 22 applies to or restricts more activity, and is, therefore, broader than Article 15 of the Data Protection Directive. Where the DPD's provisions were limited to automated decision-making connected to individual profiling—that is, processing for the purpose of "evaluat[ing] certain personal aspects" of the person—Article 22 is not limited to profiling.[101] Automated decision-making may often "partially overlap with or result from profiling[,]"[102] but the guidelines make clear that Article 22's scope goes beyond personal profiling to other kinds of automated decisions.[103]

Article 22 is also broader by virtue of being interpreted to apply to decisions involving human rubber-stamping, where several Member States had interpreted the Directive's provisions to apply only to automated decisions involving no human at all.[104] Similarly, where some Member States implemented the DPD's provisions as a right to object, the Working Party guidelines explain that Article 22 is a prohibition on algorithmic decision-making.[105] It thus applies to all automated decision-making, not just when an individual voices an objection. Thus several of the interpretations advanced by the Working Party ensure that Article 22 will apply to more activity than the DPD did.

Second, Article 22 is stronger than the Directive's provisions, meaning that it is harder law.[106] The GDPR provides both stronger penalties and stronger enforcement mechanisms.[107] And where Member States could change the

101. Mendoza & Bygrave, *supra* note 3, at 10, 11; GUIDELINES ON AUTOMATED INDIVIDUAL DECISION-MAKING, *supra* note 9, at 8 ("Automated decision-making has a different scope and may partially overlap with or result from profiling . . . Automated decisions can be made with or without profiling; profiling can take place without making automated decisions.").

102. *See* GUIDELINES ON AUTOMATED INDIVIDUAL DECISION-MAKING, *supra* note 9, at 8.

103. *See id.* (discussing example of imposing speeding fines based on evidence from speed cameras).

104. *See* GUIDELINES ON AUTOMATED INDIVIDUAL DECISION-MAKING, *supra* note 9, at 21; Wachter et al., *Why a Right to Explanation of Automated Decision-Making Does Not Exist*, *supra* note 8, at 94–95.

105. *See* GUIDELINES ON AUTOMATED INDIVIDUAL DECISION-MAKING, *supra* note 9, at 19.

106. *See, e.g.*, Kenneth W. Abbott et al., *The Concept of Legalization*, 54 INT'L ORG. 401, 404 (2000) (describing a spectrum of "legalization" along the three dimensions of obligation, precision, and delegation); Kal Raustiala & Anne-Marie Slaughter, International Law, *International Relations and Compliance*, *in* THE HANDBOOK OF INTERNATIONAL RELATIONS 538, 552 (Thomas Risse & Beth Simmons eds., 2002).

107. *See, e.g.*, Casey et al., *supra* note 8, at 165–70.

wording and in practice the meaning of the DPD through implementation, the GDPR, as a regulation, has direct effect within Member States. Thus, the wiggle room in Article 22 is lessened (even as the text still contemplates some variations by Member States) and the enforcement authority behind it is greatly strengthened.

Finally, Article 22's protections run deeper than the DPD's provisions. Specifically, the mandatory requirements for companies are more significant under the GDPR than they were under the DPD. Under the DPD, if the contract exception applied, it was not clear that a company needed to do anything else to protect individual rights—it need not necessarily adopt safeguards.[108] By contrast, Article 22 requires safeguards—even when an exception applies—that, at a minimum, include a right to human intervention, a right to object, and a right to express one's view.[109] As discussed above, the Working Party guidelines and Recitals clarify that these measures include both an individual right to explanation and multiple systemic accountability requirements such as audits.

Article 22 and the accompanying notification and access provisions in Articles 13, 14, and 15 thus put in place an algorithmic accountability regime that is broader, stronger, and deeper than the largely symbolic regime that existed under the DPD. Accompanied by other company duties in the GDPR—including establishing data protection officers, using data protection impact assessments, and following the principles of data protection by design—this regime, if enforced, has the potential to be a sea change in how algorithmic decision-making is regulated in the EU.[110]

---

108. *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) art. 15(2)(a)

> [I]s taken in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard his legitimate interests, such as arrangements allowing him to put his point of view.

109. *See* GDPR, *supra* note 6, at art. 22(3).

110. *See* Casey et al., *supra* note 8, at 173–88 (describing data protection impact assessments and data protection by design and by default); *see also* Edwards & Veale, *Slave to the Algorithm*, *supra* note 8, at 23, 68–80 (identifying the GDPR's actual algorithmic accountability regime as consisting of DPIAs, PbD, and other individual GDPR rights such as the right to erasure).

V. THE RIGHT TO EXPLANATION, REVISITED

Against this backdrop of the GDPR's strengthened algorithmic accountability regime, this Article now returns to the much-debated right to explanation. Transparency is a basic principle of the GDPR.[111] In fact, it can be striking to a U.S. audience just how many of the GDPR's rights resemble open government laws, rather than traditional privacy causes of action.[112] This is because data protection regimes are grounded in fairness, and transparency and fairness are linked ideals; we often use transparency as an element of accountability, to establish that systems are fair.[113] But in the right to explanation debate, the centrality of transparency to the GDPR has gotten lost. Several scholars have, pessimistically, vastly underrepresented what kinds of disclosures about algorithmic decision-making are required under the GDPR.[114] To be fair, these scholars largely wrote before the Working Party guidelines were finalized. But now that the final version of the guidelines has been released, some explanation of explanation is overdue.

To understand what is at stake, it is worth briefly summarizing the back-and-forth over transparency that has taken place in the literature. Scholars on both sides of the Atlantic have called for transparency in algorithmic decision-making, in the form of both notice towards individuals and audits that enable expert third-party oversight.[115] Some of these calls for transparency have been

111. *See* GDPR, *supra* note 6, at art. 5(1)(a); GUIDELINES ON AUTOMATED INDIVIDUAL DECISION-MAKING, *supra* note 9, at 9 ("Transparency of processing is a fundamental requirement of the GDPR.").

112. *Compare, e.g.*, GDPR, *supra* note 6, at arts. 12–15, *with* the U.S. Privacy Act, 5 U.S.C. § 552(a) (comparing the GDPR's rights of transparency, notification, and access to the U.S. Privacy Act, which provides individual rights of transparency into public systems of records). *Compare, e.g.*, the GDPRs implementation of the Fair Information Practice Principles (FIPS), *with* the Prosser privacy torts. For an overview of the FIPS, see GDPR, *supra* note 6, at art. 5. *See also* GDPR, *supra* note 6, Recital 39. For a discussion of the Prosser torts, see Neil M. Richards & Daniel J. Solove, *Prosser's Privacy Law: A Mixed Legacy*, 98 CALIF. L. REV. 1887, 1891–903 (2010).

113. Robert Gellman, *Fair Information Practices: A Basic History* (Apr. 10, 2017) (unpublished manuscript) (explaining the principles of transparency and fairness that are at the base of worldwide data protection regimes); *see* ORG. FOR ECON. CO-OPERATION & DEV., THE OECD PRIVACY FRAMEWORK 15 (Sept. 23, 1980, *revised* 2013) ("Openness Principle" and "Individual Participation Principle": "An individual should have the right: a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him").

114. *See, e.g.*, Edwards & Veale, *Slave to the Algorithm*, *supra* note 8; Wachter et al., *Counterfactual*, *supra* note 8; Wachter et al., *Why a Right to Explanation of Automated Decision-Making Does Not Exist*, *supra* note 8.

115. *See, e.g.*, Citron, *supra* note 1, at 1305; Citron & Pasquale, *supra* note 1; Crawford & Schultz, *supra* note 1; Hildebrandt, *supra* note 1; Kim, *supra* note 1; FRANK PASQUALE, THE

ambitiously deep and broad, suggesting that both algorithmic source code and data sets should be subjected to public scrutiny.[116] Others have responded by enumerating the harms this level of transparency could cause,[117] or by arguing that transparency directed at individuals will be relatively useless since individuals lack the expertise to do much with it.[118] But transparency of some kind has a clear place in algorithmic accountability governance, from recent calls for algorithmic impact assessments to proposals for whistleblower protections, to regularly repeated calls for algorithmic auditing.[119]

The GDPR comes closest to creating what Frank Pasquale has called "qualified transparency": a system of targeted revelations of different degrees of depth and scope aimed at different recipients.[120] Transparency in practice is not limited to revelations to the public.[121] It includes putting in place internal company oversight, oversight by regulators, oversight by third parties, and

---

BLACK BOX SOCIETY 140–88 (2015) (calling this "qualified transparency"—"limiting revelations in order to respect all the interests involved in a given piece of information").

116. Citron *supra* note 1, at 1308; Citron & Pasquale, *supra* note 1, at 20, 26 (the "logics of predictive scoring systems should be open to public inspection"). Citron & Pasquale also note that information about the datasets (but not the datasets themselves) could be released to the public. *Id.* at 27 (noting that Zarsky says the public could be informed about datasets without social risk); Zarsky, *supra* note 1, at 1563.

117. Ananny & Crawford, *supra* note 1, at 978 ("[F]ull transparency can do great harm."); Kroll et al., *supra* note 1, at 639; Zarsky, *supra* note 1, at 1553–63.

118. Edwards & Veale, *Slave to the Algorithm*, *supra* note 8, at 64, 67 ("Individuals are mostly too time-poor, resource-poor, and lacking in the necessary expertise to meaningfully make use of these individual rights."); Kroll et al., *supra* note 1, at 638 ("The source code of computer systems is illegible to nonexperts.").

119. *See, e.g.*, Desai & Kroll, *supra* note 1 (calling for whistleblower protections); A. Michael Froomkin, *Regulating Mass Surveillance as Privacy Pollution: Learning from Environmental Impact Statements*, 2015 U. ILL. L. REV. 1713, 1713 (2015) (calling for "requirements for those conducting mass surveillance in and through public spaces to disclose their plans publicly via an updated form of environmental impact statement"); Price, *supra* note 1, at 421 (arguing that the FDA should pursue a "more adaptive regulatory approach with requirements that developers disclose information underlying their algorithms"); Andrew D. Selbst, *Disparate Impact in Big Data Policing*, 52 GA. L. REV. 109 (2017) (describing the potential benefits of "algorithmic impact statements [requiring] police departments to evaluate the efficacy and potential discriminatory effects of all available choices for predictive policing technologies"); David Wright & Charles D. Raab, *Constructing a Surveillance Impact Assessment*, 28 COMPUTER L. & SECURITY REV. 613 (2012) (describing "surveillance impact assessment (SIA), a methodology for identifying, assessing and resolving risks . . . posed by the development of surveillance systems").

120. PASQUALE, *supra* note 115, at 142.

121. *See* Zarksy, *supra* note 1, at 1532 ("Intuitively, transparency is linked to merely one meaning—that the relevant information is disseminated broadly to (1) the *general public*" but "[f]ully understanding this concept, however, calls for distinguishing among the *recipients* of the information transparency policy provides."). *But see* Kroll et al., *supra* note 1, which appears to define transparency only as disclosure to the public.

communications to affected individuals. Each of these revelations may be of a different depth or kind; an oversight board might get access to the source code, while an individual instead might get clearly communicated summaries that she can understand.

To summarize the right to explanation and accompanying transparency measures, as some have, as a "transparency fallacy"—palliative measures requiring mere icons or simplistic explanations—is to both misrepresent their actual substance and mischaracterize the GDPR's overall transparency regime.[122] The GDPR's individual transparency provisions are deeper than some have suggested. And the overall accountability regime that the GDPR puts in place establishes multiple layers of transparency, some of which go very deep indeed. This Part starts with individual transparency rights, before turning to the systemic approach to algorithmic accountability that the GDPR puts in place.

Individuals have a "right to be informed" about algorithmic decision-making.[123] That right is housed both in the "meaningful information about the logic involved" provisions of Articles 13 and 14 and in Article 22(3)'s suitable safeguards provision.[124] It is true that the guidelines state that individuals need not be provided with source code or complex mathematical explanations, under either Article 22 or the accompanying notification and access provisions.[125] But that is because those individual transparency provisions are meant to serve the purpose of providing expert oversight.

The "who" and "why" of transparency in the GDPR dictates the what, when, and how. Individual transparency provisions, as the guidelines make clear, are intended to empower individuals to invoke their other rights under the GDPR.[126] Therefore, while individuals need not be provided with source code, they should be given far more than a one-sentence overview of how an algorithmic decision-making system works. They need to be given enough information to be able to understand what they are agreeing to (if a company

122. Edwards & Veale, *Slave to the Algorithm*, *supra* note 8, at 43; Wachter et. al, *Counterfactual*, *supra* note 8, at 865–66, 887.

123. GUIDELINES ON AUTOMATED INDIVIDUAL DECISION-MAKING, *supra* note 9, at 20.

124. *Id.* at 20, 25 ("Providing this information will also help controllers ensure they are meeting some of the required safeguards referred to in Article 22(3) and Recital 71.").

125. *Id.* at 25 ("[N]ot necessarily a complex explanation of the algorithms used or disclosure of the full algorithm."), 31 ("Instead of providing a complex mathematical explanation about how algorithms or machine-learning work, the controller should consider using clear and comprehensive ways to deliver the information to the data subject.").

126. *Id.* at 27 ("The controller should provide the data subject with general information . . . which is also useful for him or her to challenge the decision . . . . The data subject will only be able to challenge a decision or express their view if they fully understand how it has been made and on what basis.").

is relying on the explicit consent exception);[127] to contest a decision;[128] and to find and correct erroneous information, including inferences.[129]

Scholars have (in this Article's view, disingenuously) suggested that the GDPR's transparency requirements in Article 12—requirements that companies make an effort to communicate information in a way understandable to individuals— restrict the depth and quality of information a company must reveal.[130] Article 12 demands that companies communicate clearly, to ensure that individuals can in fact act on the information they receive. It aims to prevent companies from flooding individuals with useless or unnecessarily complicated or time-wasting information, abusing notice requirements to create obscurity through information floods.[131] In other words, Article 12 requires that companies make their communications to individuals comprehensible. It does *not* reduce the GDPR's substantial disclosure requirements to meaninglessly high-level or simplistic information

127. *Id.* at 13 ("Controllers seeking to rely upon consent as a basis for profiling will need to show that data subjects understand exactly what they are consenting to.").

128. *Id.* at 27.

129. *Id.* at 17–18 ("Individuals may wish to challenge the accuracy of the data used and any grouping or category that has been applied to them. This rights to rectification and erasure apply to both the 'input personal data' (the personal data used to create a profile), and the 'output data' (the profile itself or 'score' assigned to the person)."), 31 ("Controllers providing data subjects with access to their profile in connection with their Article 15 rights should allow them the opportunity to update or amend any inaccuracies in the data or profile.").

130. *See* Wachter et. al, *Counterfactual*, *supra* note 8, at 865 ("Detailed information appears to not be necessary as Art. 12(7) states that the required information can be provided along with standardi[z]ed icons . . . proposed icons reveal the initial expectations of regulators for simple, easily understood information."), 866 ("[E]ach provision suggests that information disclosures need to be tailored to their audience, with envisioned audiences including children and uneducated laypeople."), 887 (illustrating simplistic transparency infographics that were ultimately not adopted by the European Parliament, and stating that these "reveal the level of complexity expected by EU legislators" in an explanation to a data subject and that "[t]he reliance on generic icons suggests that individual-level, contextualised information is not required").

131. *See* Ananny & Crawford, *supra* note 1, at 979 ("[*S*]*trategic opacity*—in which actors 'bound by transparency regulations' purposefully make so much information 'visible that unimportant pieces of information will take so much time and effort to sift through that receivers will be distracted from the central information the actor wishes to conceal.' "); Zarsky, *supra* note 1, at 1508 ("The process of merely flooding the public with facts and figures does not effectively promote transparency. It might even backfire."); *see also* Wendy E. Wagner, *Administrative Law, Filter Failure, and Information Capture*, 59 DUKE L.J. 1321, 1324–25 (2010); GUIDELINES ON AUTOMATED INDIVIDUAL DECISION-MAKING, *supra* note 9, at 31 ("Instead of providing a complex mathematical explanation . . . the controller should consider using clear and comprehensive ways to deliver the information to the data subject.").

or infographics. Companies can be required to communicate in-depth information at the same time that they are required to communicate it clearly.[132]

Communication to individuals about algorithmic decision-making must thus be simultaneously understandable (or "legible"),[133] meaningful, and actionable. It must be understandable to individuals, rather than delivered in complex jargon or as an information flood.[134] However, it must also convey considerable depth; the guidelines note that "[c]omplexity is no excuse for failing to provide information."[135] And it must provide enough information that an individual can act on it—to contest a decision, or to correct inaccuracies, or to request erasure.[136]

Thus, there is a clear relationship between the other individual rights the GDPR establishes—contestation, correction, and erasure—and the kind of individualized transparency it requires. This suggests something interesting about transparency: the substance of other underlying legal rights often determines transparency's substance.[137] If one has a right of correction, one needs to see errors. If one has a right against discrimination, one needs to see what factors are used in a decision. Otherwise, information asymmetries render underlying rights effectively void.

The guidelines list examples of what kinds of information should be provided to individuals and how it should be provided. Individuals should be told both the categories of data used in an algorithmic decision-making process and an explanation of why these categories are considered relevant.[138]

---

132. *See, e.g.*, RANDALL MUNROE, THING EXPLAINER: COMPLICATED STUFF IN SIMPLE WORDS (2015) (Munroe "used line drawings and only the thousand (or, rather, "ten hundred") most common words to provide simple explanations for some of the most interesting stuff there is"). Thanks to Matthew R. Cushing for the pointer.

133. Malgieri & Comandé, *supra* note 1, at 245 (introducing the concept of legibility to this debate: "legibility is concerned with making data and analytics algorithms both transparent and comprehensible") (citing Richard Mortier, et al., *Human Data Interaction: The Human Face of the Data-Driven Society*, MIT TECH. REV. (2014); *see* Zarsky, *supra* note 1, at 1520 (discussing the related concept of interpretability).

134. GUIDELINES ON AUTOMATED INDIVIDUAL DECISION-MAKING, *supra* note 9, at 31 ("[C]lear and comprehensive").

135. *Id.* at 25, n.40.

136. *See id.* at 17, 27, 31; *see also* Mendoza & Bygrave, *supra* note 3, at 16 (explaining that the possibility of a "right of ex post explanation of automated decision is implicit in the right 'to consent' a decision"); Selbst & Powles, *supra* note 8, at 242 (explaining that enhancing data subject rights to include the right to "contest a decision" is reinforced by "GDPR's emphasis on meaningful transparency . . . in a way that is useful, intelligible, and actionable to the data subject").

137. Selbst & Barocas, *Intuitive Appeal*, *supra* note 3, at 1120–21.

138. GUIDELINES ON AUTOMATED INDIVIDUAL DECISION-MAKING, *supra* note 9, at 31 (explaining good practice recommendations for data controllers).

Moreover, they should be told the "factors taken into account for the decision-making process, and . . . their respective 'weight' on an aggregate level . . . ."[139] They should be told how a profile used in algorithmic decision-making is built, "including any statistics used in the analysis[,]"[140] and the sources of the data in the profile.[141] Lastly, companies should provide individuals an explanation of why a profile is relevant to the decision-making process and how it is used for a decision.[142]

The GDPR's individualized system of algorithmic transparency thus requires far more than a counterfactual explanation (e.g., "if you were not 25, you would have gotten this job").[143] The guidelines further note, in several places, that companies should use technological design to create more effective notice mechanisms, such as through "visuali[z]ation and interactive techniques."[144] Not only is it a company's duty to communicate a particular depth of information, but a company must also pay attention to using effective design choices to ensure that information is both noticed and understood.

This does not mean that the individual right to explanation and the accompanying transparency rights in the GDPR give individuals a right to all information about an algorithm. Nor does it mean to suggest that the conversation about what information must be released to individuals ends here. It is clear from the guidelines that this conversation will be ongoing. There is still room to read in, for example, a best practice of releasing performance metrics, which the guidelines do not suggest.[145] Two scholars have proposed a number of suggestions of the kind of information that would be useful—including both information about the model (the family of model, training parameters, summary input data, human-understandable averages of how inputs become outputs, how the model was tested, trained, or screened) and information about the individual decision (counterfactuals, which cases

139. *Id.* at 27 ("[W]hich is also useful for him or her to challenge the decision.").

140. *Id.* at 31.

141. *Id.*

142. *See id.*

143. *But see* Wachter et. al, *Counterfactual*, *supra* note 8.

144. GUIDELINES ON AUTOMATED INDIVIDUAL DECISION-MAKING, *supra* note 9, at 31 ("Controllers may want to consider implementing a mechanism for data subjects to check their profile, including details of the information and sources used to develop it."). *Id.* at 32 ("Controllers could consider introducing online preference management tools such as a privacy dashboard."). Hildebrandt, *supra* note 1, at 53 (calling for "TETs": transparency-enhancing tools); Citron & Pasquale, *supra* note 1, at 29 (suggesting interactive modeling).

145. Edwards & Veale, *Slave to the Algorithm*, *supra* note 8, at 55; Malgieri & Comandé, *supra* note 8, at 259.

are most similar to the individual's, what characteristics cause individuals to receive similar treatment, how confident the system is of a specific outcome).[146]

But the GDPR's individual algorithmic transparency rights, accompanied by other GDPR transparency rights, go a long way towards establishing what U.S. scholars have called for—including revealing the sources of data, inferences about an individual, and even some math.[147] Throughout, the emphasis is on individual understanding of information of a meaningful depth, so that an individual subject of algorithmic decision-making can invoke her rights.

Other forms of systemic transparency that go substantially deeper accompany this individualized transparency regime. Individuals might not have access to source code or datasets, but other parties do. The GDPR's regime of systemic transparency is established through Article 22's safeguards provision and the Working Party interpretation of it, and through more general GDPR provisions such as the requirement of impact assessments.[148] This systemic transparency regime includes the requirement of data protection impact assessments for automated processing, the general information-forcing and oversight powers granted to regulatory authorities.

There are a number of ways that systematic transparency can be implemented. First, regulators can use significant information-forcing capabilities under the GDPR to get access to information about algorithms.[149] The GDPR also envisions general data protection audits conducted by government authorities.[150]

Second, most companies deploying algorithmic decision-making must set up internal accountability and disclosure regimes. They must perform a data protection impact assessment,151 and provide information to an internal but

146. Edwards & Veale, *Slave to the Algorithm*, *supra* note 8, at 55–56, 58.

147. GUIDELINES ON AUTOMATED INDIVIDUAL DECISION-MAKING, *supra* note 9, at 31 (mentioning "any statistics used in the analysis").

148. *Id.* at 28, 32 (discussing safeguards under art. 22). GDPR, *supra* note 6, at art. 35, art. 58.

149. GDPR, *supra* note 6, at art. 58(1)(e) (authorizing the authority to carry out data protection audits, and "obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks").

150. *See id.* at art. 58(1)(b).

151. *Id.* at art. 35(3)(a) (requiring a data protection impact assessment "in a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person"); GUIDELINES ON AUTOMATED INDIVIDUAL DECISION-MAKING, *supra* note 9, at 29–30 (explaining that this requirement "will apply in the case of decision-making including profiling

independent data protection officer who has, at least on paper, deep information-forcing abilities.[152] Companies that fall under Article 22 must also give human reviewers deeper transparency onto "all the relevant data" as part of the right to human intervention.[153]

Third, the guidelines suggest that companies performing decision-making with a "high impact on individuals" should use independent third-party auditing and provide that auditor with "all necessary information about how the algorithm or machine learning system works."[154] Hence, the GDPR's approach to systemic accountability establishes a second aspect of Pasquale's "qualified transparency": deeper information flows, including source code, both within companies and to regulatory authorities and third-parties. It is true that this information does not get released to the public. But it is myopic to focus only on the individual version of transparency and decry its shallowness, rather than seeing its place and purpose in a system of required information flows.

The purpose of each transparency measure affects not just the depth of information revealed but also the timing of transparency.[155] Discrete events in the GDPR trigger individual transparency—when, for example, data is collected,[156] a decision is made,[157] an individual's consent is obtained,[158] or an individual requests information.[159] This connects individualized transparency to the rights of an individual, but limits the efficacy of individualized transparency at creating oversight over the construction of an algorithm, or its ongoing performance. In particular, individual transparency rights largely occur after the fact of algorithmic development, when it is far more difficult (if not impossible) to impose accountability or corrections on a system.[160] By

with legal or similarly significant effects that is not wholly automated, as well as solely automated decision-making defined in Article 22(1)").

152. *Id.* at art. 38(2) ("The controller and processor shall support the data protection officer in performing the tasks . . . by providing . . . access to personal data and processing operations . . . ."); GUIDELINES ON AUTOMATED INDIVIDUAL DECISION-MAKING, *supra* note 9, at 29–30.

153. GUIDELINES ON AUTOMATED INDIVIDUAL DECISION-MAKING, *supra* note 9, at 27 (assess "all the relevant data").

154. *Id.* at 32.

155. Ananny & Crawford, *supra* note 1, at 982 (discussing the "temporal dimension of transparency").

156. *See* GDPR, *supra* note 6, at arts. 13, 14.

157. *See id.* at art. 22; GDPR, *supra* note 6, Recital 71.

158. GUIDELINES ON AUTOMATED INDIVIDUAL DECISION-MAKING, *supra* note 9, at 12–13.

159. GDPR, *supra* note 6, at art. 15

160. Kroll et al., *supra* note 1 at 659–60, 662; Desai & Kroll, *supra* note 1 at 39–42.

contrast, the GDPR's systemic accountability measures are envisioned as ongoing, continuous,[161] and being implemented early on in an algorithm's development. This creates, in theory at least, internal, expert/third-party, and regulatory oversight over the development of an algorithm from its inception, better serving the purposes of correcting error, inaccuracy, and bias in a changing system over time.

VI. CONCLUSION

The GDPR sets up a system of "qualified transparency" over algorithmic decision-making that gives individuals one kind of information, and experts and regulators another. This multi-pronged approach to transparency should not be dismissed as lightly as some have done. There is an individual right to explanation. It is deeper than counterfactuals or a shallow and broad systemic overview, and it is coupled with other transparency measures that go towards providing both third-party and regulatory oversight over algorithmic decision-making. These transparency provisions are just one way in which the GDPR's system of algorithmic accountability is potentially broader, deeper, and stronger than the previous EU regime.

It is one thing to put these requirements on paper and quite another to have them operate in practice. The system of algorithmic accountability that the GDPR and its accompanying interpretative documents envision faces significant hurdles in implementation: high costs to both companies and regulators, limited individual access to justice, and limited technical capacity of both individuals and regulators. As I note elsewhere, there are other ways in which the GDPR may fail.[162] Its heavy reliance on collaborative governance in the absence of significant public or third-party oversight could lead to capture or underrepresentation of individual rights.[163]

But for companies with a footprint in the EU, it is important to note that the GDPR does govern algorithmic decision-making, and many of the

161. *See, e.g.*, GUIDELINES ON AUTOMATED INDIVIDUAL DECISION-MAKING, *supra* note 9, at 28

> Controllers should introduce appropriate procedures and measures to prevent errors, inaccuracies or discrimination on the basis of special category data. These measures should be used on a cyclical basis; not only at the design stage, but also continuously, as the profiling is applied to individuals. The outcome of such testing should feed back into the system design.

See, e.g., Ananny & Crawford, *supra* note 1, at 976.

162. *See* Kaminski, *Binary Governance*, *supra* note 3, at 67–68.

163. *See, e.g.*, CHRISTINA ANGELOPOULOS ET AL., STUDY OF FUNDAMENTAL RIGHTS LIMITATIONS FOR ONLINE ENFORCEMENT THROUGH SELF-REGULATION (2016) (discussing the problems raised by delegating individual rights protection to companies).

potential loopholes in that system have been limited or closed. Companies face a decision of whether to put humans meaningfully back in the loop of algorithmic decision-making and thus escape Article 22. Otherwise, they must put in place a significant set of safeguards, including both individual rights and ongoing internal and third-party accountability measures.