COLUMBIA LAW REVIEW

VOL. 121 NOVEMBER 2021 NO. 7

ARTICLES

THE RIGHT TO CONTEST AI

Margot E. Kaminski & Jennifer M. Urban***

Artificial intelligence (AI) is increasingly used to make important decisions, from university admissions selections to loan determinations to the distribution of COVID-19 vaccines. These uses of AI raise a host of concerns about discrimination, accuracy, fairness, and accountability.

In the United States, recent proposals for regulating AI focus largely on ex ante and systemic governance. This Article argues instead—or really, in addition—for an individual right to contest AI decisions, modeled on due process but adapted for the digital age. The European Union, in fact, recognizes such a right, and a growing number of institutions around the world now call for its establishment. This Article argues that despite considerable differences between the United States and other countries, establishing the right to contest AI decisions here would be in keeping with a long tradition of due process theory.

This Article then fills a gap in the literature, establishing a theoretical scaffolding for discussing what a right to contest should look like in practice. This Article establishes four contestation archetypes that should serve as the bases of discussions of contestation both for the right to contest AI and in other policy contexts. The contestation archetypes vary along two axes: from contestation rules to standards and from emphasizing procedure to establishing substantive rights. This Article then discusses four processes that illustrate these archetypes in practice, including the first in-

* Associate Professor of Law, University of Colorado Law School, Director of the Privacy Initiative at Silicon Flatirons.

** Clinical Professor of Law, Director of Policy Initiatives for the Samuelson Law, Technology & Public Policy Clinic; Co-Director, Berkeley Center for Law and Technology. Opinions are our own and should not be attributed to our respective institutions. Urban's opinions also should not be attributed to the California Privacy Protection Agency or the California Privacy Protection Agency Board. Thank you to Tal Zarsky and contributing commentators at Privacy Law Scholars Conference (PLSC), to the faculty at Colorado Law, the University of Washington, and the University of California, Berkeley for workshopping, and to Ifeoma Ajunwa, Ignacio Cofone, Catherine Fisk, Aziz Huq, Sonia Katyal, Christopher Kutz, Michael Brian Lang, Orly Lobel, Przemysław Pałka, Dylan Penningroth, Richard Re, Blake Reid, Pierre Schlag, Jonathan Simon, Scott Skinner-Thompson, Erik Stallman, Harry Surden, and Rebecca Wexler for thoughts on drafts. We are particularly grateful to Paul Schwartz and his students for advice on revisions. Mistakes are our own.

depth consideration of the GDPR's right to contestation for a U.S. audience. Finally, this Article integrates findings from these investigations to develop normative and practical guidance for establishing a right to contest AI.

INTRODUCTION

What appeals rights, if any, should people have when they are subjected to decision-making by artificial intelligence (AI)?[1] The right to challenge decisions with significant effects is a core principle of the rule of

1. For purposes of discussion, this Article uses "AI" decision-making as a shorthand to refer to decision-making by algorithms more generally. Though computer scientists would not consider all of the algorithms used for decision-making today to qualify as artificial intelligence, decision-making algorithms are rapidly growing more sophisticated. See, e.g., Harry Surden, Artificial Intelligence and Law: An Overview, 35 Ga. St. U. L. Rev. 1305, 1307 (2019) (indicating the range of applications to which decision-making algorithms have been applied, including playing chess and driving vehicles). More practically, even relatively simple algorithms can be used to substitute, in whole or in part, for human decision-making—an extension, or replacement, of human intelligence. Id. at 1335 ("[Legal self-help systems] are simple expert systems—often in the form of chatbots—that provide ordinary users with answers to basic legal questions.").

It is helpful, though, to consider the background behind the shorthand. An algorithm is a computer program. E.g., David Lehr & Paul Ohm, Playing With the Data: What Legal Scholars Should Learn About Machine Learning, 51 U.C. Davis L. Rev. 653, 660–61 (2017). There are many different kinds of algorithms of varying levels of autonomy and sophistication, some of which are collectively referred to as AI: These range from programs that automate fields of human expertise by mapping out what human experts know, to algorithms that scan vast amounts of data, to algorithms that, effectively, create their own rules. See, e.g., Surden, supra, at 1310 (dividing AI into (1) machine learning and (2) logical rules and knowledge representation). Algorithmic decision-making entails using a computer program to make a decision. This can mean taking the decision a computer program gives you as the end result or relying on such a decision as a significant element in human decision-making. See, e.g., Algorithmic Accountability Act, S. 1108, 116th Cong. § 2(1) (2019) (defining an automated decision system as "a computational process . . . , that makes a decision or facilitates human decision making, that impacts consumers").

The EU's recently proposed Artificial Intelligence Act (AIA) similarly defines "AI" expansively. The draft AIA defines an "AI system" as "software that is developed with one or more of the techniques and approaches listed in Annex I," which include (a) machine-learning approaches, (b) logic- and knowledge-based approaches, and (c) statistical approaches, and that "can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they

law.[2] Yet it is unclear how this principle will fare for significant decisions made or facilitated by AI.

As data collection and storage have become cheaper, processing has become faster, and algorithms have become more complex and more effective at certain tasks, the use of AI in decision-making has increased. The government and private sector now use algorithms to decide how to distribute welfare benefits,[3] whether to hire or fire a person,[4] whether expressive material should be removed from online platforms,[5] whether to keep people in prison,[6] and more.[7]

The increasing use of AI to aid or substitute for human decision-making raises the question of what, if any, process should be afforded those affected by these decisions.[8] Machine decision-making can be technically

---

interact with." European Commission, Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, at tit. I art. 3(1), annex I, COM (2021) 206 final (Apr. 21, 2021).

2. See, e.g., Henry J. Friendly, "Some Kind of Hearing", 123 U. Pa. L. Rev. 1267 (1975) ("The Court has consistently held that some kind of hearing is required at some time before a person is finally deprived of his property interests." (quoting Wolff v. McDonnell, 418 U.S. 539, 557–58 (1974))).

3. See, e.g., Danielle Keats Citron, Technological Due Process, 85 Wash. U. L. Rev. 1249, 1252 (2008) [hereinafter Citron, Technological Due Process]; see also Ryan Calo & Danielle Keats Citron, The Automated Administrative State: A Crisis of Legitimacy, 70 Emory L.J. 797, 800–01 (2021); David Freeman Engstrom, Daniel E. Ho, Catherine M. Sharkey & Mariano-Florentino Cuéllar, Government by Algorithm: Artificial Intelligence in Federal Administrative Agencies 17 (2020), https://www-cdn.law.stanford.edu/wp-content/uploads/2020/02/ACUS-AI-Report.pdf [https://perma.cc/Q5G5-X24E] (showcasing that AI is used, among other things, in social welfare policy).

4. See Ifeoma Ajunwa, An Auditing Imperative for Automated Hiring Systems, 34 Harv. J.L. & Tech. 621, 631–33 (2021) [hereinafter Ajunwa, Auditing Imperative]; Ifeoma Ajunwa, The Paradox of Automation as Anti-Bias Intervention, 41 Cardozo L. Rev. 1671, 1694 (2020) [hereinafter Ajunwa, Paradox of Automation] (citing the example of Goldman Sachs building an algorithmic model to automate all management, including hiring and firing); Pauline T. Kim, Data-Driven Discrimination at Work, 58 Wm. & Mary L. Rev. 857, 860 (2017).

5. See Rory Van Loo, Federal Rules of Platform Procedure, 88 U. Chi. L. Rev. 829, 836–37 (2021) (discussing the processes used by technology platforms to resolve disputes); infra notes 312–313 and accompanying text.

6. See, e.g., Jessica M. Eaglin, Constructing Recidivism Risk, 67 Emory L.J. 59, 61 (2017); Deirdre K. Mulligan & Kenneth A. Bamberger, Procurement as Policy: Administrative Process for Machine Learning, 34 Berkeley Tech. L.J. 773, 776 (2019); Rebecca Wexler, Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System, 70 Stan. L. Rev. 1343, 1348 (2018).

7. See, e.g., Mulligan & Bamberger, supra note 6, at 784–85 (collecting examples of government use of algorithmic decision-making, including determining veterans' disability compensation; evaluating teachers and determining their compensation; identifying children at risk of abuse or neglect; and allocating public services).

8. See, e.g., Danielle Keats Citron & Frank Pasquale, The Scored Society: Due Process for Automated Predictions, 89 Wash. L. Rev. 1, 27 (2014) [hereinafter Citron & Pasquale, Scored Society]; Citron, Technological Due Process, supra note 3, at 1281; Kate Crawford & Jason Schultz, Big Data and Due Process: Toward a Framework to Redress Predictive Privacy

inscrutable and thus difficult to contest; it is likely to become even less scrutable as black-box machine-learning techniques expand.[9] Humans may exhibit an "automation bias" that creates overconfidence in machine decisions,[10] and an ensuing bias against challenges to those decisions.[11] It is unclear how challenges, especially if they come with meaningful process rights, will affect the cost efficiencies that automated decision-making promises to deliver. And if related due process protections such as transparency and notice are implemented badly or not at all, meaningful challenges will not be possible.

In the United States, regulatory proposals directed at algorithmic decision-making have largely ignored calls for individual due process in favor of system-wide regulation aimed at risk mitigation. To the extent there has been convergence among recent U.S. policy proposals, it has been on the need for systemic policy solutions, such as algorithmic impact assessments or auditing, rather than an individual right to contest.[12]

Harms, 55 B.C. L. Rev. 93, 109 (2014); Aziz Z. Huq, A Right to a Human Decision, 106 Va. L. Rev. 611, 651 (2020) [hereinafter Huq, A Right to a Human Decision]; Aziz Z. Huq, Constitutional Rights in the Machine-Learning State, 105 Cornell L. Rev. 1875, 1905 (2020) [hereinafter Huq, Constitutional Rights in the Machine-Learning State].

9. 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'y 973, 981–82 (2016); Jenna Burrell, How the Machine 'Thinks': Understanding Opacity in Machine Learning Algorithms, Big Data & Soc'y Jan.–June 2016, at 3 ("At the heart of this challenge is an opacity that relates to the specific techniques used in machine learning."); Tal Zarsky, The Trouble With Algorithmic Decisions: An Analytic Road Map to Examine Efficiency and Fairness in Automated and Opaque Decision Making, 41 Sci. Tech. & Hum. Values 118, 123–27 (2016) [hereinafter Zarsky, The Trouble With Algorithmic Decisions]. See generally Emre Bayamlıoğlu, Transparency of Automated Decisions in the GDPR: An Attempt for Systemisation 17 (Jan. 16, 2018) (unpublished manuscript) (on file with the *Columbia Law Review*) [hereinafter Bayamlıoğlu, Transparency of Automated Decisions] ("Automated data-driven systems are distinguished by their complex, increasingly autonomous, and adaptive properties which render their technical dimension and inner workings obscure to human cognition."); Tal Z. Zarsky, Transparent Predictions, 2013 U. Ill. L. Rev. 1503 [hereinafter Zarsky, Transparent Predictions] (describing the importance of transparency and advancing a framework for understanding the role it must play in AI regulation).

10. Lee A. Bygrave, Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling, 17 Comput. L. & Sec. Rep. 17, 18 (2001) [hereinafter Bygrave, Minding the Machine] (describing humans' "automatic acceptance of the validity of the decisions reached"); Citron, Technological Due Process, supra note 3, at 1271–72; Isak Mendoza & Lee A. Bygrave, The Right Not to Be Subject to Automated Decisions Based on Profiling, *in* EU Internet Law 77, 83 (Tatiani-Eleni Synodinou, Philippe Jougleux, Christiana Markou & Thalia Prastitou eds., 2017) ("The Commission . . . expressed a fear that such processes will cause humans to take for granted the validity of the decisions reached and thereby reduce their own responsibilities to investigate and determine the matters involved.").

11. See, e.g., Citron, Technological Due Process, supra note 3, at 1271–72.

12. See, e.g., Algorithm Accountability Act of 2019, S. 1108, 116th Cong. (2019); H.R. 1655, 66th Leg., 2019 Reg. Sess. (Wash. 2019) (explaining that the act, "[r]elating to establishing guidelines for government procurement and use of automated decision systems," attempts to establish "algorithmic accountability report[s]"); Margot E. Kaminski, Binary Governance: Lessons From the GDPR's Approach to Algorithmic Accountability, 92 S. Cal.

In Europe, by contrast, regulators are taking a more holistic approach to algorithmic decision-making. The European Union's (EU) General Data Protection Regulation (GDPR), which went into effect in May 2018, establishes a complex set of regulations of algorithmic decision-making that span multiple contexts and sectors.[13] The GDPR incorporates both systemic governance measures and various individual rights for data subjects: transparency, notice, access, a right to object to processing, and, for those subject to automated decision-making, the *right to contest* certain decisions.[14]

Likewise, the Council of Europe has articulated a right to contest in its amended data protection convention, known as Convention 108.[15] The Council of Europe is an international human rights organization that consists of all the EU Member States plus additional non-EU members.[16] As of now, forty countries have signed on to the amended Convention.[17] Twelve have ratified it.[18] The amended Convention states that "[e]very individual shall have a right[] . . . not to be subject to a decision significantly affecting him or her based solely on an automated processing of data without *having his or her views taken into consideration.*"[19] In 2020, the Council of Europe adopted recommendations on AI, explaining that individuals should be

---

L. Rev. 1529, 1582–1607 (2019) [hereinafter Kaminski, Binary Governance] (contrasting and analyzing the GDPR's interplay between individual rights and collaborative governance) [hereinafter Kaminski, Binary Governance]. But see California's newly enacted amendment to the California Consumer Privacy Act (CCPA), the California Privacy Rights Act (CPRA), which includes a provision on individual rights requiring the California Privacy Protection Agency to issue

> regulations governing access and opt-out rights with respect to businesses' use of automated decisionmaking technology, including profiling and requiring businesses' response to access requests to include meaningful information about the logic involved in those decisionmaking processes, as well as a description of the likely outcome of the process with respect to the consumer.

Cal. Civ. Code § 1798.185(16) (2020).

13. See Commission Regulation 2016/679, 2016 O.J. (L 119/1) 1 (EU) [hereinafter GDPR]; Kaminski, Binary Governance, supra note 12, at 1538–40 (comparing human and algorithmic decision-making).

14. See GDPR, supra note 13, art. 22(3).

15. Council of Eur., Convention 108+: Convention for the Protection of Individuals With Regard to Automatic Processing of Personal Data 15 (2018), https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1 [https://perma.cc/N5DL-DUWQ] [hereinafter Convention 108].

16. Id. at 34.

17. Modernisation of the Data Protection "Convention 108", Council of Eur., https://www.coe.int/en/web/portal/28-january-data-protection-day-factsheet [https://perma.cc/C5FR-HK7E] (last visited July 31, 2021).

18. Italy, a 12th Ratification for Convention 108+, Council of Eur. (July 8, 2021), https://www.coe.int/en/web/data-protection/-/italy-a-12th-ratification-for-convention-10-1 [https://perma.cc/P8TN-7CCS].

19. Convention 108, supra note 15, art. 9(1)(a) (emphasis added).

provided "effective *means to contest* relevant determinations and decisions."[20]

The right to contest AI is developing traction outside of Europe, too. The Organisation for Economic Co-operation and Development (OECD), an intergovernmental economic organization focused on stimulating world trade, includes a right to contest in its recommendations on AI.[21] The OECD's recommendations have historically formed the basis of data protection laws around the world, and its recommendations on AI are likely to be similarly influential. Brazil's comprehensive data protection law, enacted in 2018, includes "the right to request a review of decisions taken" by AI.[22] In November 2020, the Office of the Privacy Commissioner of Canada recommended that Canadian data privacy law be revised to include a right to contest AI decisions.[23] The proposed amendments to Quebec's privacy law, Bill 64, include a limited right to contest.[24]

Despite this, few have given attention to the right to contest AI. Although the GDPR's notice and transparency requirements for AI, especially the so-called "right to explanation," have attracted a flurry of scholarly analysis,[25] contestation has not garnered as much attention.[26] And although the right to contest is clearly established in the GDPR, regulators

20. Council of Eur., Recommendation CM/Rec(2020)1 of the Committee of Ministers to Member States on the Human Rights Impacts of Algorithmic Systems 9, 13 (2020) https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016809e1154 [https://perma.cc/YC8H-QUTX] [hereinafter Council of Eur., Recommendation on the Human Rights Impacts of Algorithmic Systems] (emphasis added).

21. OECD, Recommendation of the Council on Artificial Intelligence, § 1.3.iv, OECD Legal Instruments (May 5, 2019), https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449 (on file with the *Columbia Law Review*).

22. See General Personal Data Protection Act (LGPD), Law No. 13,709, art. 20, 2018, https://lgpd-brazil.info/chapter_03/article_20 [https://perma.cc/W2CL-SFTW] (Braz.).

23. A Regulatory Framework for AI: Recommendations for PIPEDA Reform, Off. of the Priv. Comm'r of Can., (Nov. 2020), https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-ai/reg-fw_202011/ [https://perma.cc/E6ZL-AP7H]; see also Ignacio Cofone, Policy Proposals for PIPEDA Reform to Address Artificial Intelligence Report, Off. of the Priv. Comm'r of Can. (Nov. 2020), https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-ai/pol-ai_202011/#fn190-rf [https://perma.cc/Y4MH-YZ2X] (last updated Nov. 12, 2020).

24. An Act to Modernize Legislative Provisions as Regards the Protection of Personal Information, National Assembly of Québec, Bill 64, 102.12.1, 102.12.1(3) (2020) (Can.). In addition to the right to correct erroneous information used to arrive at the decision, "[t]he person concerned must be given the opportunity to submit observations to a member of the personnel of the enterprise who is in a position to review the decision." Id.

25. See, e.g., Margot E. Kaminski, The Right to Explanation, Explained, 34 Berkeley Tech. L.J. 189, 192 n.8 (2019) [hereinafter Kaminski, Right to Explanation, Explained] (citing literature).

26. A minority of European scholars have discussed contestation. See Mireille Hildebrandt, Privacy as Protection of the Incomputable Self: From Agnostic to Agonistic Machine Learning, 20 Theoretical Inquiries L. 83, 119–20 (2019) [hereinafter Hildebrandt,

have yet to give meaningful guidance on what the right is or how it should be implemented.

This Article takes on the right to contest, both descriptively and normatively. It seeks to fill the gap in commentary and bridge the U.S. and EU conversations. This Article is the first to examine at length this right and its content, and the first to provide an in-depth analysis of the GDPR right to contestation for a U.S. audience.[27]

This Article investigates a central question about regulating algorithmic decision-making: Should there be a right to contest AI decisions? In investigating this question, this Article uncovers and fills a substantial gap in the literature: the lack of a theoretical scaffolding for discussing contestation models for privatized process at speed and at scale. This Article probes this question theoretically, considering reasons frequently given for establishing individual due process rights, and comparatively, through in-depth case studies of existing contestation systems. Ultimately, we find merit in the possibility of establishing a right to contest AI, including

---

Privacy as Protection of the Incomputable Self] ("This should result in testable and contestable decision-systems whose human overlords can be called to account, squarely facing the legal interpretability problem and its relationship with the computer science interpretability problem."); Mireille Hildebrandt, The Dawn of a Critical Transparency Right for the Profiling Era, *in* Digital Enlightenment Yearbook 2012, at 41, 49–54 (Jacques Bus Malcolm Crompton, Mireille Hildebrandt & George Metakides eds., 2012); Mendoza & Bygrave, supra note 10, at 93–94 ("[A] right of contest is not simply a matter of being able to say 'stop', but is akin to a right of appeal . . . . [T]o be meaningful, it must set . . . an obligation to hear and consider the merits of the appeal . . . . [I]t must additionally . . . provide . . . reasons for the decision.").

27. Related work that touches on the right to contest includes Emre Bayamlıoğlu, Contesting Automated Decisions: A View of Transparency Implications, 4 Eur. Data Prot. L. Rev. 433, 433–35 (2018) [hereinafter Bayamlıoğlu, Contesting Automated Decisions] (discussing transparency requirements for effective contestation of automated decisions from a European perspective); Bayamlıoğlu, Transparency of Automated Decisions, supra note 9, at 3–4, 17 (proposing a transparency framework from a European perspective); Huq, A Right to a Human Decision, supra note 8, at 621–22 (interpreting Article 22 as establishing a "right to a human decision," and rejecting such a right). In an article arguing for counterfactuals as a method of providing the "explanation" required by Recital 71 of the GDPR, Sandra Wachter, Brent Mittelstadt, and Chris Russell assert that these explanatory counterfactuals could support contestation rights. Sandra Wachter, Brent Mittelstadt & Chris Russell, Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR, 31 Harv. J.L. & Tech. 841, 872–78 (2018) [hereinafter Wachter et al., Counterfactual Explanations Without Opening the Black Box].

Deirdre K. Mulligan and coauthors have developed the related concept of "contestable design": system design that encourages and allows iterative human engagement in a system's evolution and deployment. Contestable design operates differently from ex post contestation, but systems designed for contestability could support contestation in practice. See, e.g., Daniel Kluttz, Nitin Kohli & Deirdre K. Mulligan, Shaping Our Tools: Contestability as a Means to Promote Responsible Algorithmic Decision Making in the Professions, *in* After the Digital Tornado: Networks, Algorithms, Humanity 137, 139 (Kevin Webach ed., 2020); Daniel N. Kluttz & Deirdre K. Mulligan, Automated Decision Support Technologies and the Legal Profession, 34 Berkeley Tech. L.J. 861 (2019); Mulligan & Bamberger, supra note 6, at 791, 850–57.

where decisions are made by private actors, to further due process values. We consider how to design an effective right.

Part I introduces some of the challenges algorithmic decision-making presents and how they might relate to contestation. Part II turns to whether a right to contest AI decision-making can find theoretical purchase. Part III looks to models for contestation, establishing four contestation archetypes and examining them in action through comparative case studies. It considers the GDPR's right to contest and Member State implementations of it, the Digital Millennium Copyright Act's "notice-and-takedown" scheme for online copyright infringement, the Fair Credit Billing Act's contestation scheme for credit card charges, and the EU's so-called "right to be forgotten." Part IV integrates the findings from these investigations and develops normative and practical guidance for designing a right to contest AI.

I. AI DECISION-MAKING: KNOWN PROBLEMS AND CONTESTATION AS A POSSIBLE SOLUTION

On March 23, 2020, the International Baccalaureate Organization (IBO) canceled spring exams in response to the COVID-19 pandemic.[28] More than 170,000 students in nearly 150 countries[29] faced this final hurdle in their two-year journey toward an International Baccalaureate (IB) Diploma—a credential used by universities around the world to determine admissions and scholarships and to award advanced course credits.[30] In lieu of exams, the IBO chose to evaluate students using an algorithm.[31]

On July 6, the IBO released final "grades," to international uproar.[32] Many students discovered that their grades were lower than they and their

28. May 2020 Examinations Will No Longer Be Held, Int'l Baccalaureate Org. (Mar. 23, 2020), https://www.ibo.org/news/news-about-the-ib/may-2020-examinations-will-no-longer-be-held/ [https://perma.cc/ZY2C-ALTU].

29. Int'l Baccalaureate Org., The IB Diploma Programme Final Statistical Bulletin: May 2020 Assessment Session 2 (2020), https://www.ibo.org/contentassets/bc850970f4e54b87828f83c7976a4db6/dp-statistical-bulletin-may-2020-en.pdf [https://perma.cc/W2EJ-HVUP].

30. University Admission, Int'l Baccalaureate Org., https://www.ibo.org/university-admission/ [https://perma.cc/84UW-GV6R] (last visited July 31, 2021).

31. The IBO announced that it would employ a "method that uses data, both historical and from the present session, to arrive at the subject grades for each student," and that it would be "undertaking significant data analysis" as part of "a rigorous process of due diligence in what is a truly unprecedented situation." The Assessment and Awarding Model for the Diploma Programme May 2020 Session, Int'l Baccalaureate Org. (May 13, 2020), https://www.ibo.org/news/news-about-ib-schools/the-assessment-and-awarding-model-for-the-diploma-programme-may-2020-session/ [https://perma.cc/5TBD-36LP].

32. See, e.g., Anam Rizvi, International Baccalaureate Organisation Defends Awarding Model After Backlash from Pupils, National (July 15, 2020), https://www.thenational.ae/uae/education/international-baccalaureate-organisation-defends-awarding-model-after-backlash-from-pupils-1.1049550/ [https://perma.cc/9F3H-FQHA]; Tom Simonite, Meet the Secret Algorithm That's Keeping Students Out of College, WIRED (July 10, 2020), https://www.wired.com/story/algorithm-set-students-grades-altered-futures/ [https://perma

teachers had expected.[33] Some students lost scholarships, leaving them uncertain how to pay for college.[34] Others feared losing provisional acceptances to universities.[35] In Colorado, Isabel Castaneda's "heart sank" when she saw that she had failed a number of IB courses, including high-level Spanish, her native language. In an interview, Castaneda said, "I come from a low-income family—and my entire last two years were driven by the goal of getting as many college credits as I could to save money on school."[36]

By July, more than 15,000 students and parents had signed an online petition asserting that the magnitude of downgrading some students experienced "is . . . blatant evidence of a faulty algorithm."[37] The IBO updated grades based on feedback it received but ultimately stood by its method.[38] The IBO refused to answer questions about its system, which it characterized as an "IB awarding model, not a computer-based algorithm."[39] The IBO stated, however, that the model combined completed coursework, predictive grades, and "school context" to determine grades.[40]

All of this only raised more red flags for critics. It suggested that students from historically poorer-performing schools could be disadvantaged, and that this would disproportionately harm students from

---

.cc/QYM4-53EG] [hereinafter Simonite, Meet the Secret Algorithm] (last updated July 13, 2020).

33. Chan Ho-him, Number of Hong Kong Students With Perfect Scores in International Baccalaureate Drops by Nearly a Third After Grading System Change Amid Pandemic, S. China Morning Post (July 6, 2020), https://www.scmp.com/news/hong-kong/education/article/3092054/number-hong-kong-students-perfect-scores-international/ [https://perma.cc/NMX9-RV6T]; see also Simonite, Meet the Secret Algorithm, supra note 32 (explaining that several students received results much lower than expected by their teachers).

34. Simonite, Meet the Secret Algorithm, supra note 32.

35. Id.

36. Avi Asher-Schapiro, Global Exam Grading Algorithm Under Fire for Suspected Bias, Reuters (July 21, 2020), https://www.reuters.com/article/us-global-tech-education-analysis-trfn/global-exam-grading-algorithm-under-fire-for-suspected-bias-idUSKCN24M29L/ [https://perma.cc/7YLM-GNX2].

37. Ali Zagmout, Justice for May 2020 IB Graduates—Build a Better Future! #IBSCANDAL, Change.org, https://www.change.org/p/international-baccalaureate-organisation-ibo-justice-for-may-2020-ib-graduates-build-a-better-future/ [https://perma.cc/952Z-88VH] (last visited July 31, 2021).

38. Int'l Baccalaureate Org., supra note 29, at 1.

39. Awarding May 2020 Results Further Information, Int'l Baccalaureate Org. (Mar. 23, 2020), https://www.ibo.org/news/news-about-the-ib/awarding-may-2020-results-further-information [https://perma.cc/57NU-WRVN]; see also Simonite, Meet the Secret Algorithm, supra note 32. Experts considered this characterization implausible. See Asher-Schapiro, supra note 36.

40. Asher-Schapiro, supra note 36. According to a statement by the IB, a "school's own record was built into the model," which used "historical data to model predicted grade accuracy, as well as the record of the school to do better or worse on examinations compared with coursework." Id. For schools with little historical data, IB would use data pooled from other schools. Simonite, Meet the Secret Algorithm, supra note 32.

historically marginalized groups.[41] Others pointed out that a school's record might not be a reliable indicator for individual students, pointing to the surprisingly large drops from predictive to final grade that some students experienced as evidence that the statistical model was inaccurate for individuals.[42]

At first, the IBO offered only its usual appeals route or for students to retake exams in November, both of which require paying fees.[43] On July 14, the IBO relented to an extent by making changes to its appeals process.[44] It still did not release details about its decision-making system, leaving open the question of how students and universities could know whether the grading model was accurate or fair.[45] A recent article in the *Harvard Business Review* notes that "what the IBO could have done instead was offer appellants the right to a human-led re-evaluation of anomalous grades, specify what input data the appeal committee would focus on in reanalyzing the case, and explain how the problem would be fixed."[46] In other words, the IBO could have afforded students a right to contest the algorithm.

The IBO's decision to use an algorithm to determine important outcomes for a class of people is far from uncommon today. Indeed, the IB controversy is not the only algorithmic grading controversy. In England, Wales, and Northern Ireland, officials also responded to the pandemic by using an algorithm to grade the exams taken by university-bound students.[47] Met with vehement opposition when nearly 40% of students were assigned lower grades than predicted,[48] education officials reverted to the predicted grades.[49]

---

41. Asher-Schapiro, supra note 36. The student and parent petition expressed that the average grades masked and exacerbated this inequality, arguing that "[t]he global average has increased obviously due to the fact that certain schools around the world achieved much higher grades than before." Zagmout, supra note 37.

42. Scott Jaschik, What's Wrong With This Year's IB Scores?, Inside Higher Ed (July 13, 2020), https://www.insidehighered.com/admissions/article/2020/07/13/algorithm-used-ib-scores-year-blamed-students-low-marks/ [https://perma.cc/6268-XH8E].

43. Simonite, Meet the Secret Algorithm, supra note 32.

44. Catherine Lough, Exclusive: IB 'Concession' Over Grade Appeals, Tes (July 14, 2020), https://www.tes.com/news/coronavirus-ib-concession-over-grades-welcomed-head teachers [https://perma.cc/D7CK-RR22] (reporting that the IB changed its appeals process to "make[] it potentially easier for students to receive higher grades if they appeal against their results").

45. Theodoros Evgeniou, David R. Hardoon & Anton Ovchinnikov, What Happens When AI Is Used to Set Grades?, Harv. Bus. Rev. (Aug. 13, 2020), https://hbr.org/2020/08/what-happens-when-ai-is-used-to-set-grades/ [https://perma.cc/E2PG-495U] (noting that, "[s]ince the specifics of the program are not disclosed, all people can see are the results").

46. Id.

47. A-Levels and GCSEs: How Did the Exam Algorithm Work?, BBC (Aug. 20, 2020), https://www.bbc.com/news/explainers-53807730 [https://perma.cc/28WT-9YS5].

48. Matt Burgess, The Lessons We All Must Learn From the A-Levels Algorithm Debacle, WIRED (Aug. 20, 2020), https://www.wired.co.uk/article/gcse-results-alevels-algorithm-explained [https://perma.cc/G8NE-4FMB].

49. A-Levels and GCSEs: How Did the Exam Algorithm Work?, supra note 47.

As important as entrance-exam grades are for students, even more significant decisions are now entrusted to algorithms. Both the public and private sectors now regularly delegate decision-making to AI. Algorithms have been used for employment decisions,[50] welfare benefits distribution and denials,[51] policing,[52] housing advertisements,[53] risk assessments at criminal sentencing,[54] COVID-19 vaccine allocation,[55] and home-health-care resources,[56] among many other applications.

The use of AI is growing in large part because of efficiency: AI can be cheaper and faster than human decision-makers. It may be the only viable

---

50. Ajunwa, Auditing Imperative, supra note 4, at 631–40 (discussing "the business case for the trend toward automated hiring," noting "the potential for automated hiring systems to be misused to produce unlawful employment discrimination," and describing how such systems may serve to mask employment discrimination or impede its detection"); Ajunwa, Paradox of Automation, supra note 4, at 1692–704 ("The automation of the hiring process represents a particularly important technological trend and one that requires greater legal attention given its potential for employment discrimination."); Kim, supra note 4, at 867–92 (considering "the potential for data models to eliminate" bias in the workplace).

51. Calo & Citron, supra note 3, at 799–801 (explaining that Idaho and Michigan are among the states whose agencies have used flawed systems to automate public-benefits determinations); Citron, Technological Due Process, supra note 3, at 1256 (recounting how the Colorado Benefits Management System issues thousands of incorrect eligibility determinations and benefit calculations, many as a result of coding errors); Engstrom et al., supra note 3, at 17 (explaining that a study of AI and machine learning in U.S. federal agencies found social welfare agencies to have the fourth-highest number of use cases).

52. Andrew Guthrie Ferguson, The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement 18–19 (2017) ("Big data tools create the potential for big data policing.").

53. See Charge of Discrimination, Facebook, FHEO No. 01-18-0323-8, slip op. ¶¶ 7–21 (Mar. 28, 2019) (alleging that Facebook "uses machine learning and other prediction techniques to classify and group users" to determine the audience for advertisements, including housing advertisements).

54. See Eaglin, supra note 6, at 67–88 (observing that "the use of actuarial tools heralds a new, data-centric approach to prediction in sentencing"); Mulligan & Bamberger, supra note 6, at 776–77 (discussing a case involving the constitutionality of risk assessment software used in sentencing in Wisconsin); Wexler, supra note 6, at 1348 (observing that "[r]isk assessment instruments are among the most controversial" automated criminal justice technologies).

55. Noah Weiland, At a National Kickoff Event, Officials Plead With the Public to Get Vaccinated, N.Y. Times (Dec. 14, 2020), https://www.nytimes.com/live/2020/12/14/world/covid-19-coronavirus/ (on file with the *Columbia Law Review*) (last updated Jan. 4, 2021) ("The five people were selected by an algorithm the hospital used to assign the first doses, the result of a survey hospital employees filled out that asked about age and underlying medical conditions."); see also Lenny Bernstein, Lateshia Beachum & Hannah Knowles, Stanford Apologizes for Coronavirus Vaccine Plan That Left Out Many Front-Line Doctors, Wash. Post (Dec. 18, 2020), https://www.washingtonpost.com/health/2020/12/18/stanford-hospital-protest-covid-vaccine/ (on file with the *Columbia Law Review*).

56. See Erin McCormick, What Happened When a 'Wildly Irrational' Algorithm Made Crucial Healthcare Decisions, Guardian (July 2, 2021), https://www.theguardian.com/us-news/2021/jul/02/algorithm-crucial-healthcare-decisions/ [https://perma.cc/67MD-SDDP] (explaining the effects of an algorithm the state of Idaho created to apportion home care assistance).

option when decisions must be made at scale.[57] Proponents also claim that algorithms can be fairer, less biased, and more accurate than human decision-makers.[58] Indeed, despite substantial evidence of mistakes and discriminatory effects,[59] scholars see an unsettling tendency for humans to place excessive trust in algorithmic decisions,[60] tempted by what Paul Schwartz in 1992 called the "seductive precision" of computational outputs.[61] There is evidence that human decision-makers may rely more readily on these machine decisions, trusting them as "objective" even when they are not.[62]

But AI is not always accurate and does not eliminate human bias. In some cases, it instead obfuscates bias with layers of ostensibly objective mathematical authority. As the IBO example and others illustrate, the use of and reliance on AI for significant decision-making raises a host of concerns about inaccuracy, bias, discrimination, and other errors. For example, an algorithm used to allocate home-health-care resources in multiple U.S. states failed to take into account important aspects of patients' situations—including whether they had diabetes or cerebral palsy—resulting in cuts in care, "incalculable human suffering," and death.[63] An algorithm used by the Mass General Brigham health system to estimate kidney func-

57. See, e.g., infra note 358 and accompanying text (describing how receiving millions or billions of copyright takedown notices impels online service providers to implement algorithmic processing systems).

58. E.g., Jane Bambauer & Tal Zarsky, The Algorithm Game, 94 Notre Dame L. Rev. 1, 7–8 (2018); Huq, A Right to a Human Decision, supra note 8, at 654–55.

59. See, e.g., Virginia Eubanks, Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor 168 (2018) (describing machines' lack of empathy); Andrew D. Selbst, Disparate Impact in Big Data Policing, 52 Ga. L. Rev. 109, 120–21 (2017) [hereinafter Selbst, Disparate Impact in Big Data Policing] (noting examples of algorithm use with discriminatory outcomes).

60. See Bygrave, Minding the Machine, supra note 10, at 18 (observing that the European Commission expressed a fear that "the increasing automatisation of decision-making processes engenders automatic acceptance of the validity of the decisions reached and a concomitant reduction in the investigatory and decisional responsibilities of humans"); Citron, Technological Due Process, supra note 3, at 1271–72 (observing that "[t]he cognitive system's engineering literature has found that human beings view automated systems as error-resistant" and that "[o]perators of automated systems tend to trust a computer's answers"); Mendoza & Bygrave, supra note 10, at 83 ("The Commission also expressed anxieties over the quality of fully automated decision-making processes, more specifically a fear that such processes will cause humans to take for granted the validity of the decisions reached . . . .").

61. Paul Schwartz, Data Processing and Government Administration: The Failure of the American Legal Response to the Computer, 43 Hastings L.J. 1321, 1341–42 (1992) (attributing the computer's "seductive precision" to "the difference between the power that we attribute to it and its actual capacities and limitations").

62. See Citron, Technological Due Process, supra note 3, at 1271–72 ("Studies show that human beings rely on automated decisions even when they suspect system malfunction.").

63. McCormick, supra note 56.

tion assigned Black people healthier scores than it assigned to white people with similar kidney function, leaving Black patients less likely to be referred to a specialist or referred for a kidney transplant.[64] Amazon's AI recruiting tool consistently assigned women a lower score than men.[65] The Apple Card's creditworthiness algorithm has been accused of giving women lower credit limits.[66]

Biased outcomes like these do not necessarily occur because the programmers of algorithms intend to discriminate. A study of facial recognition software led by an MIT researcher revealed that baked-in bias from training data (that primarily included white men) predictably resulted in biased decisions (that failed, for example, to accurately recognize Black women).[67] Algorithms also reflect programmer decisions that implicate substantive values, from what model programmers choose to deploy to how they choose to weigh false positives versus false negatives.[68]

These issues apply across a range of technologies. Concerns about inaccuracy, bias, and discrimination are raised even by relatively simple actuarial algorithms—that is, statistically derived algorithms—used in criminal sentencing.[69] More complex machine-learning algorithms present additional challenging and important questions about transparency and accountability.[70] Some black-box algorithms cannot be assessed ex

---

64. See Tom Simonite, How an Algorithm Blocked Kidney Transplants to Black Patients, WIRED (Oct. 26, 2020), https://www.wired.com/story/how-algorithm-blocked-kidney-transplants-black-patients/ [https://perma.cc/QYW5-Y8SS] [hereinafter Simonite, Kidney Transplants]. If the same formula used for white patients had been used for Black patients, a full third of Black patients—more than 700 people—would have had their kidney disease classified into a more severe category. Id.

65. See Jeffrey Dastin, Amazon Scraps Secret AI Recruiting Tool That Showed Bias Against Women, Reuters (Oct. 10, 2018), https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G/ [https://perma.cc/V2S7-K4FP] ("[Amazon's system] penalized resumes that included the word 'women's,' as in 'women's chess club captain.'").

66. See Evelina Nedlund, Apple Card Is Accused of Gender Bias. Here's How That Can Happen, CNN Bus. (Nov. 12, 2019), https://www.cnn.com/2019/11/12/business/apple-card-gender-bias/index.html/ [https://perma.cc/4U6T-RH3X].

67. See Larry Hardesty, Study Finds Gender and Skin-Type Bias in Commercial Artificial-Intelligence Systems, MIT (Feb. 11, 2018), https://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212/ [https://perma.cc/E36B-S5VP].

68. See generally U.S. Dept. of Health, Educ. & Welfare, Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems 23 (1973) [hereinafter HEW Report] ("[A] serious[] consequence of putting record keeping in the hands of a new class of data-processing specialists is that questions . . . which involve issues of social policy are sometimes treated as if they were nothing more than questions of efficient technique."); Citron, Technological Due Process, supra note 3, at 1267 (describing programmers' substantive policy decisions); Lehr & Ohm, supra note 1 (explaining how the benefit and harm "of choosing certain machine-learning algorithms is the ability to place weight on particular types of errors over others").

69. Eaglin, supra note 6, at 68–69 n.41.

70. See, e.g., Solon Barocas & Andrew D. Selbst, Big Data's Disparate Impact, 104 Calif. L. Rev. 671, 674 (2016) [hereinafter Barocas & Selbst, Big Data's Disparate Impact]

post to determine how decisions were made, and programming decisions can distort policy in application.[71]

At the limit, AI decision-making can raise concerns about "what it means to be human."[72] In both the private sector and public sector contexts, human decision-makers who might employ discretion, exercise compassion, tailor statistics to a specific application, or otherwise apply human expertise are being removed from the decisional loop.[73] Eliminating human decision-makers and replacing them with a machine arguably affects the dignity of the human subject of the decision.[74] As an attorney for home-health-care patients whose care was cut by a new algorithmic decision-making system put it, "we move into unsettling territory when we rely solely upon algorithms and data to make determinations about health care needs . . . . We reduce a person's humanity to a number."[75]

This is not to say that human decision-makers are necessarily better than algorithms. The same human who introduces compassion can also introduce error or bias. Human judges can be racist, both explicitly and implicitly.[76] Discrimination by a human decision-maker can also harm the dignity of a human subject.

("[B]ecause the mechanism through which data mining may disadvantage protected classes is less obvious in cases of unintentional discrimination, the injustice may be harder to identify and address."); Crawford & Schultz, supra note 8, at 108 (describing the privacy risk that may arise due to the complex nature of Big Data); Lehr & Ohm, supra note 1, at 705–10 (laying out the importance of increasing the explainability of AI to reduce potential bias); Surden, supra note 1, at 1311–12 ("[A]lgorithms improve their performance by examining more data and detecting additional patterns in that data that assist in making better automated decisions.").

71. Citron, Technological Due Process, supra note 3, at 1261 ("Policy is often distorted when programmers translate it into code.").

72. Meg Leta Jones, The Right to a Human in the Loop: Political Constructions of Computer Automation and Personhood, 47 Soc. Stud. Sci. 216, 219 (2017) [hereinafter Jones, The Right to a Human in the Loop].

73. See, e.g., Rebecca Crootof, "Cyborg Justice" and the Risk of Technological-Legal Lock-In, 119 Colum. L. Rev. Forum 233, 236 (2019) (comparing human judges to AI judges); A. Michael Froomkin, Ian Kerr & Joelle Pineau, When AIs Outperform Doctors: Confronting the Challenges of a Tort-Induced Over-Reliance on Machine Learning, 61 Ariz. L. Rev. 33, 37 (2019) ("The reduction in new data from physicians . . . creates scenarios in which we cannot rule out the risk that sub-optimal conclusions are reached."); Mulligan & Bamberger, supra note 6, at 791 (describing how the algorithmic system used in the food stamp program resulted in a discriminatory effect).

74. See Jones, The Right to a Human in the Loop, supra note 72, at 219 ("[T]echnological developments . . . significantly challenge our notions of human agency and autonomy—what it means to be human in light of computational technical advances like artificial intelligence and robotics."); Zarsky, The Trouble With Algorithmic Decisions, supra note 9, at 129 ("Algorithmic decision-making processes raise . . . autonomy-related concerns that also involve harms to individual dignity.").

75. McCormick, supra note 56.

76. E.g., Justin D. Levinson, Forgotten Racial Equality: Implicit Bias, Decisionmaking, and Misremembering, 57 Duke L.J. 345, 350 (2007); Gregory Scott Parks, Judging Racism, 2012 Cardozo L. Rev. de novo 238, 246–47, https://ssrn.com/abstract=3004078 [https://perma.cc/8SYU-VDE3].

The shift from human decision-making to AI or hybrid human–AI decision-making systems, however, decisively alters the policy landscape and thus affects social values.[77] For example, instead of having a human decision-maker evaluate a particular individual's particular circumstances ex post, AI decision-making shifts some policy decisions early on to the designers of an algorithm.[78] In some cases, other policy decisions are shifted into the "black box" of the algorithm itself, unobservable, perhaps, even to the designers. *Who* makes decisions and *when* decisions are made change. This can affect both the outcome of decisions and accountability, as parts of the decision-making process become less visible. If a doctor tells you that you have not been recommended for a kidney transplant, you can ask why. If AI makes the decision, you can't (currently) ask the programmer to explain it.[79] As one patient whose home health care was drastically cut by an algorithm described, neither she nor the assessor who entered her data into the program could "quite understand what was happening."[80] In addition, at least one third-party software vendor implementing the algorithm simply didn't know that the program improperly accounted for diabetes, saying, "As far as we knew, we were doing it the right way."[81]

A shift to AI decision-making can entail, too, a shift to *categorically based* decisions instead of individual tailoring.[82] This leads to what has been referred to as the long-tail problem, where an AI inappropriately applies familiar categories to "[w]eird stuff that's hard to deal with."[83] For example, a self-driving car trained to avoid cats, dogs, and deer can be incapable of "seeing" kangaroos in the road.[84] The USDA's fraud alert algorithm for food stamps (SNAP) that was trained to alert for fraud on whole-number

77. See Meg Leta Jones, Ironies of Automation Law: Tying Policy Knots With Fair Automation Practices Principles, 18 Vand. J. Ent. & Tech. L. 77, 88–92 (2015) (explaining the inherent flaws and risks of automation); see also Kaminski, Binary Governance, supra note 12, at 1538–40 (comparing human and algorithmic decision-making).

78. See Citron, Technological Due Process, supra note 3, at 1261 ("Code writers also interpret policy when they translate it from human language to computer code."); Eaglin, supra note 6, at 88 ("Tools constructed to estimate recidivism risk reflect numerous normative choices.").

79. See generally Andrea Roth, Machine Testimony, 126 Yale L.J. 1972 (2017) (offering a framework for conceptualizing and regulating machine evidence).

80. Colin Lecher, What Happens When an Algorithm Cuts Your Health Care, Verge (Mar. 21, 2018), https://www.theverge.com/2018/3/21/17144260/healthcare-medicaid-algorithm-arkansas-cerebral-palsy/ (on file with the *Columbia Law Review*).

81. Id.

82. Kaminski, Binary Governance, supra note 12, at 1538–40 ("Algorithmic decision-making can be biased, reflecting biased decisions made by programmers or historic discrimination baked into the data sets on which algorithms are trained."); see also Crootof, supra note 73, at 236.

83. Evan Ackerman, Autonomous Vehicles vs. Kangaroos: The Long Furry Tail of Unlikely Events, IEEE Spectrum (July 5, 2017), https://spectrum.ieee.org/cars-that-think/transportation/self-driving/autonomous-cars-vs-kangaroos-the-long-furry-tail-of-unlikely-events [https://perma.cc/S27X-7RBT].

84. Id.

purchases mistakenly identified fraud at Somali-American grocers, where customers would purchase meat in whole-dollar amounts.[85] In practice, the "long tail" can include things that aren't "weird" in any objective sense: For example, the error-prone home-health-care allocation algorithms failed to appropriately consider diabetes or cerebral palsy, hardly outlier conditions.[86]

All this is to say: Human decision-making may not always be better than AI decision-making. But AI decision-making raises distinct challenges to our assumptions about how decision-making works, which in turn structure how we have regulated—or not regulated—decision-making.

A. *A Right to Contest AI Decisions*

As the use of AI decision-making grows, so does the importance of addressing the challenges it presents. As discussed below, some U.S. scholars have responded to these concerns with calls for updated procedural and substantive protections designed to address the risks created by algorithmic decision-making.[87] One tool for addressing bad AI decisions, gaining traction in some parts of the world but largely ignored in the United States, is contestation: giving individuals affected by AI decisions the right to challenge those decisions.

Contestation is a core mechanism for establishing and preserving justice in the Western adversarial tradition. The right takes many forms. Sometimes it appears within a broader adversarial process. For example, criminal defendants have the right to confront witnesses against them,[88] and civil defendants have the right to reply to plaintiffs' complaints and make counter-claims. Sometimes it requires the provision of "some kind

85. H. Claire Brown, How an Algorithm Kicks Small Businesses Out of the Food Stamps Program on Dubious Fraud Charges, Counter (Oct. 8, 2018), https://thecounter.org/usda-algorithm-food-stamp-snap-fraud-small-businesses/ [https://perma.cc/UEZ7-GYFH]; Chris McGann, Somali Grocers Lose Right to Use Food Stamps, Seattle PI (Apr. 8, 2002), https://www.seattlepi.com/news/article/Somali-grocers-lose-right-to-use-food-stamps-1084746.php/ [https://perma.cc/GPZ3-LPLN].

86. See Lecher, supra note 80; McCormick, supra note 56.

87. See infra section I.D.

88. The right to confront witnesses was established in the United States by the Sixth Amendment. As Frank R. Herrmann and Brownlow M. Speer establish, the confrontation right extends back at least 1,500 years and probably much further. Frank R. Herrmann & Brownlow M. Speer, Facing the Accuser: Ancient and Medieval Precursors of the Confrontation Clause, 34 Va. J. Int'l L. 481, 483 (1994). It can be found in recognizable form in legislation of Emperor Justinian from 539 CE. As the Supreme Court noted in *Coy v. Iowa*, Acts 25:16, which was composed between the years 80 CE and 90 CE, quotes a Roman general explaining that the prisoner Paul will be afforded customary Roman confrontation rights. The same rights were described by Cicero in 70 BCE. Id. at 482–83. As noted infra section II.A.1, it is also found in the even more ancient Book of Proverbs, which teaches, "The one who first states a case seems right, until the other comes and cross-examines." Proverbs 18:17 (NSRV).

of" process for challenging a decision—i.e., the contestation itself, effected.[89] Accordingly, in the United States, administrative decisions with significant effects may be subject to appeal and are generally subject to the recipient's "opportunity to be heard."[90] Similarly, in the EU, the "right to be heard" is considered a fundamental principle that both Member States and individual citizens are guaranteed.[91] Nor are contestation rights confined to government decisions. Both legislatures[92] and courts[93] have imposed some forms of contestation (and other due process) responsibilities on private companies.

The right to contest decisions is central to due process. Indeed, other familiar due process protections—for example, transparency, notice, and the right to an impartial arbiter—serve to strengthen contestation rights. The U.S. Constitution guarantees additional procedural protections for individuals, such as the right to trial by jury, and the right to counsel, which allow individuals to contest certain decisions with serious ramifications.[94] As Part II discusses below, contestation, in turn, serves to perfect more substantive rights of fairness and justice and to preserve rule of law values, by

89. Friendly, supra note 2, at 1274.

90. See id. at 1273, 1300 n.168 (collecting cases); see also, e.g., Goldberg v. Kelly, 397 U.S. 254, 267–68 (1970) (ruling that a hearing including an "effective opportunity to defend" is required before terminating welfare benefits). A sufficient "opportunity to be heard," however, does not necessarily mean an evidentiary hearing. Mathews v. Eldridge, 424 U.S. 319, 340 (1976).

91. See, e.g., Marco Borraccetti, Fair Trial, Due Process and Rights of Defence in the EU Legal Order, *in* The EU Charter of Fundamental Rights: From Declaration to Binding Instrument 95, 105–06 (Giacomo Di Federico ed., Springer 2011). Article 41 of the Charter reads:

> Every person has the right to have his or her affairs handled impartially, fairly and within a reasonable time by the institutions, bodies, offices, and agencies of the Union. This right includes: the right of every person to be heard, before any individual measure which would affect him or her adversely is taken; . . . [and] the obligation of the administration to give reasons for its decisions.

Charter of Fundamental Rights of the European Union, 2012 O.J. (C 326) 391, 403–04.

92. See, e.g., Fair Credit Reporting Act of 1970, 15 U.S.C. § 1681 (2018) (imposing dispute resolution requirements for consumer credit bureaus); Digital Millennium Copyright Act, 17 U.S.C. § 512 (2018) (imposing copyright dispute resolution responsibilities on Internet intermediaries in return for a safe harbor from secondary copyright liability).

93. See, e.g., Cotran v. Rollings Hudig Hall Int'l, Inc., 948 P.2d 412, 422 (Cal. 1998) (noting that "good cause" in the context of an implied employment contract requires an "appropriate investigation" that includes "notice of the claimed misconduct and a chance for the employee to respond"); Silva v. Lucky Stores, Inc., 76 Cal. Rptr. 2d 382, 387 (Ct. App. 1998) ("[I]nvestigative fairness contemplates listening to both sides and providing employees a fair opportunity to present their position and to correct or contradict relevant statements prejudicial to their case, without the procedural formalities of a trial." (citing *Cotran*, 948 P.2d at 422)); Jody Freeman, The Private Role in Public Governance, 75 N.Y.U. L. Rev. 543, 589 nn.184–88, 590 nn.189–90 (2000) (collecting cases).

94. See Huq, A Right to a Human Decision, supra note 8, at 625–26.

correcting errors, preventing or changing unjust outcomes, and enhancing the predictability and consistency of decisions. A fair contestation process can enhance the perceived legitimacy of both the law itself and specific outcomes.[95]

Despite this robust tradition, U.S. policymakers have largely eschewed individual rights in recently proposed laws governing AI, both at the state and federal levels.[96] By contrast, in the EU, the GDPR's Article 22 established an individual "right to contest" an AI decision, and this model has recently gained traction in Europe and beyond.

B. *The GDPR's Right to Contestation*

The GDPR's right to contestation, though largely ignored in the United States, has become increasingly influential in AI policy discussions around the world. In Article 22, the GDPR dictates that for certain automated decisions, affected individuals must be provided "at least the right to obtain human intervention . . . to express his or her point of view and *to contest the decision*."[97]

The GDPR applies to all processing of personal data (with some exceptions). Thus Article 22 applies to automated decisions that entail processing personal data, which includes many if not most AI decisions affecting individuals on an individual level.[98] The GDPR applies to both the government and the private sector.[99] The GDPR's right to contestation,

---

95. On legitimacy, see generally E. Allan Lind & Tom R. Tyler, The Social Psychology of Procedural Justice (1988) (exploring the view that people may be more interested in issues of process than issues of outcome); John Thibaut & Laurens Walker, Procedural Justice: A Psychological Analysis (1975) (offering objective data indicating that individuals feel more fairly treated in adversarial than in inquisitorial proceedings).

96. See supra note 12.

97. GDPR, supra note 13, art. 22(3) (emphasis added).

98. For AI that is not subject to the GDPR, the European Commission has recently proposed draft regulations on AI. Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, § 1.2, COM (2021) 206 final (Apr. 4, 2021), https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence/ [https://perma.cc/AG8H-FLD2]; see also Proposal for a Regulation on a European Approach for Artificial Intelligence, Legislative Train, Eur. Parl. (June 24, 2021), https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-regulation-on-artificial-intelligence/ [https://perma.cc/5X7L-2FH6] (noting that regulations on AI have been proposed and will be discussed in the European Parliament). The proposed regulations are built on risk mitigation, and do not include a right to contest AI that does not involve processing personal data. They would act, however, as an overlay on the GDPR, leaving its right to contest in place.

99. See, e.g., GDPR, supra note 13, arts. 3(1), 4(7)–(8) (stating that "[t]his Regulation applies to the processing of personal data" by a "controller or processor in the Union" and defining both "controller" and "processor" to include a "legal person, public authority, agency or other body"). The GDPR has law enforcement exceptions for things like journalism or public health research, for example. Id. art. 23(1) (providing exceptions where necessary to safeguard, among other things, national security, public security, public health

therefore, at least in theory, establishes due process rights for individuals significantly affected by many uses of AI in the EU. There are, however, several limits to its scope, discussed further below: It applies only to decisions that are "based solely on automated processing" and that have "significant[]" effects on the concerned individual.[100]

The GDPR's right to contestation has its origins in earlier European laws on automated decision-making. Prior to Europe-wide efforts to harmonize data protection laws, a subset of European countries enacted these laws as part of their data protection regimes. A French data protection law, enacted in 1978, proscribed both governmental and private decisions "based solely on any automatic processing of data which describes the profile or personality of the citizen concerned."[101] French law established an early version of algorithmic due process, stating that a "person shall be entitled to . . . *dispute the data and logic* used in automatic processing, the results of which are asserted against him."[102] Both the first Spanish data protection law and the first Portuguese data protection law contained similar provisions.[103]

The 1995 EU-wide Data Protection Directive (Directive), which preceded the GDPR, contained the direct precursor to the GDPR's right to contestation: a little-known, little-used provision on "Automated individual decisions," Article 15(2).[104] It required, in most cases where automated decision-making was permitted, that a company or a state adopt "suitable measures to safeguard [a person's] legitimate interests."[105] These "suitable measures" included "arrangements allowing [a person] . . . *to put his point*

objectives). In general, the GDPR starts from broad coverage, limited by EU "competencies" (meaning, it doesn't cover things the EU itself cannot reach, such as national security), and then carves out exceptions. This differs from U.S. sectoral privacy laws, which start by covering a particular type of information or a particular sector or particular entities.

100. Id. art. 22(1).

101. Loi 78-17 du 6. Janvier 1978 Relative à l'Informatique, aux Fichiers et aux Libertés, Section 2 of the Act, translated in Data Protection in the European Community: the Statutory Provisions (Spiros Simitis, Ulrich Dammann, Marita Körner-Dammann & Anne-Arendt eds., 1992); see also Bygrave, Minding the Machine, supra note 10, at 17 n.2.

102. Loi 78-17 du 6. Janvier 1978, § 3 (emphasis added).

103. Bygrave, Minding the Machine, supra note 10, at 17 n.3; see also Art. 12 of first Spanish law (Ley organica 5/1992 de 29. De octubre 1992, de Regulacion del Tratamiento Automatizado de los Datos de Caracter Personal; replaced and repealed by Law 15/1999 of 13.12.1999); Art. 16 of Portuguese data protection law (Lei. No. 10/91 de 12. De Abril 1991, da Proteccao de Dados Pessoais face a Informatica), replaced and repealed by Law no. 67/98 of 26.10.1998.

104. Council Directive 95/46, art. 15, 1995 O.J. (L 281) 43 (EC) [hereinafter DPD].

105. Id. arts. 15(2)(a), 15(2)(b). The one case in which an automated decision was permitted but no suitable safeguards were required was when a data subject's request for entering into a contract had been satisfied (meaning, there was a positive outcome for the data subject). See DPD, supra note 104, art. 15(2)(a); Bygrave, Minding the Machine, supra note 10, at 21.

of view" to the entity using automated decision-making.[106] Article 15, however, lacked the GDPR's explicit mention of a "right . . . to contest the decision."[107]

Lee Bygrave has noted that the Directive's Article 15 had very little effect on the ground.[108] Article 15 applied only when "a large number of conditions [were] satisfied."[109] Moreover, the Directive did not have direct effect as law, and Member State implementation of Article 15 arguably weakened it.[110] Some Member States (Austria, Belgium, Germany, and others) implemented Article 15 as a prohibition on algorithmic decision-making; others, like the United Kingdom, implemented it as a right to opt out of algorithmic decision-making.[111] The opt-out approach put the onus on individuals, few of whom invoked the right.[112] Thus Article 15, in practice, became according to Bygrave a "second-class data protection right . . . rarely enforced, poorly understood and easily circumvented."[113]

Article 22 of the GDPR supersedes the Directive's Article 15. Though the two provisions exhibit strong similarities, the GDPR's Article 22 appears to provide "broader, stronger, and deeper" protections than the Directive's Article 15.[114] One of the ways in which Article 22 is deeper—that is, provides more protections—than Article 15 is that it includes not just a right to express one's view, but a right to contest an automated decision.

Like its predecessor, the GDPR makes the right to contestation available only in limited circumstances. The right arises only in cases in which "solely" algorithmic decisions have legal or "similarly significant[]" effects on data subjects.[115] Elsewhere, one of us has discussed these restrictions in

---

106. DPD, supra note 104, art. 15(2)(a) (emphasis added).

107. GDPR, supra note 13, art. 22(3).

108. Bygrave describes it as "[a]ll dressed up but nowhere to go," and a "house of cards." Bygrave, Minding the Machine, supra note 10, at 21.

109. Id.

110. See id. at 17–18 ("[Article 15] directs each EU Member State to confer on persons a right to prevent them being subjected to such decision making. Hence, a legally adequate implementation of Art.15(1) may occur when national legislators simply provide persons with the opportunity to exercise such a right.").

111. 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 Priv. L. 76, 94–95 (2017) [hereinafter Wachter et al., Why a Right to Explanation of Automated Decision-Making Does Not Exist].

112. Id. at 95 ("If Article 22 is interpreted as a right to object, automated decision-making is restricted only to cases in which the data subject actively objects.").

113. Mendoza & Bygrave, supra note 10, at 3.

114. Kaminski, Right to Explanation, Explained, supra note 25, at 201.

115. We accept the Article 29 Working Party's view that "Article 22(1) establishes a general prohibition for decision-making based solely on automated processing," some exceptions to the general prohibition, and safeguards for the exceptions. Article 29 Data Prot. Working Party, Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679, 17/EN. WP 251rev.01, at 19 (Feb. 6, 2018) [hereinafter Guidelines on Automated Individual Decision-Making]; see also Kaminski, Right to

greater detail and has argued that Article 22's scope is nonetheless broader than the Directive's; it covers not only algorithmic decision-making but also such decision-making with some degree of human involvement. Also, Article 22 covers decision-making having a comparatively broad range of significant effects, including not just legal effects but also things like particularly manipulative targeted advertising.[116]

Article 22 begins with a general prohibition of automated decision-making with significant effects. There are, however, three exceptions: if a decision is necessary for a contract; if it is authorized by EU or Member State law; or if it is based on the data subject's *explicit* consent—a stronger form of consent than envisioned elsewhere in the GDPR.[117]

Companies that use automated decision-making under one of these exceptions are not unfettered. They must implement "suitable measures to safeguard [an individual's] rights and freedoms and legitimate interests."[118] Such safeguards 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*."[119]

Explanation, Explained, supra note 25, at 197. Beyond the Guidelines' persuasive power, we think this is the most sensible interpretation. Others, however, interpret Article 22(1) as only a "right" that the data subject must actively invoke. For a detailed account of the arguments for each interpretation, see Emily Pehrsson, The Meaning of the GDPR Article 22, at 17–22 (Stan.-Vienna Transatlantic Tech. L. F., Working Paper No. 31, 2018), https://www-cdn.law.stanford.edu/wpcontent/uploads/2018/05/pehrsson_eulawwp31.pdf [https://perma.cc/T566-EZDK].

In any event, these "limited cases" may be more common than they first appear. Article 22(2) allows automated decision-making when "necessary" to execute a contract, when it is authorized by Member State law, or when there is explicit consent, a set of exceptions that Giancarlo Malgieri characterizes as "wide and general." GDPR, supra note 13, art. 22(2); Gianclaudio Malgieri, Automated Decision-Making in the EU Member States: The Right to Explanation and Other "Suitable Safeguards" in the National Legislations, Comput. L. & Sec. Rev., Oct. 2019, at 1, 4 [hereinafter Malgieri, Automated Decision-Making in the EU Member States]. Article 23 allows Member States to create legislative exemptions to many of the GDPR's algorithmic process protections for a laundry list of purposes, such as national security, criminal and civil enforcement, ethics investigations, and "other important objectives of general public interest of the Union or a Member State." GDPR, supra note 13, art. 23(1). Further, it is still unclear at what point human involvement would exempt a decision-making process from Article 22's protections. The Guidelines on Automated Individual Decision-Making and Profiling say that a human with "authority and competence" must have an "actual influence on the result" to take a decision out of Article 22, Guidelines on Automated Individual Decision-Making, supra, at 21, but some think that "even nominal involvement of a human" would accomplish this, Wachter et al., Why a Right to Explanation of Automated Decision-Making Does Not Exist, supra note 111, at 88.

116. Kaminski, Right to Explanation, Explained, supra note 25, at 201–03.

117. GDPR, supra note 13, art. 22(2). For further discussion, see Kaminski, Right to Explanation, Explained, supra note 25, at 197–98 (explaining that both the contractual exception and the explicit consent exception could be interpreted to be broader or narrower, depending on the interpretation of when a decision is "necessary" for a contract).

118. GDPR, supra note 13, art. 22(3).

119. Id. art. 22(3) (emphasis added).

What this right to contest means is unclear from the text. It is clear, however, that the right to contest is more than a right to correct inaccurate data on which a decision is based.[120] Elsewhere, the GDPR provides general access and correction rights for data processing.[121] The right to contest must be something more than just the generally applicable right to correction.

The relationship between the three safeguards/rights named in Article 22 is also unclear. These rights—to human intervention, expression of a point of view, and contestation—could be understood independently. Or they could be understood to be redundant, naming aspects of the same envisioned process.[122]

Arguably, however, the "right to contest is the backbone" of Article 22's protections.[123] As Emre Bayamlıoğlu observes, the GDPR's new wording compared to the Directive's "points at . . . at least, an obligation to hear the merits of the appeal and to provide a justification for the decision."[124] This right "obliges the data controller either to render automated decisions contestable or to cease [automated decision-making] at all."[125] Thus other individual rights in the GDPR, including both transparency and process rights, are understood to be necessary for, or precursors to, this central right to contestation.[126]

Contestability relies on transparency—just as due process requires notice, in addition to an opportunity to be heard. The GDPR compels multiple forms of transparency, including a general right to notice of personal data processing, and a more specific right to "meaningful information about the logic involved" in automated decision-making.[127] It also contains

120. For a related query, see Sandra Wachter & Brent Mittelstadt, A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI, 2019 Colum. Bus. L. Rev. 494, 568–71 ("Although there is no consensus about the legal rights over inferences, there is an argument to be made that even the GDPR goes beyond procedural data control and management (informational self-determination), and provides safeguards against inferences and decisions based on inferences with the right to contest in Article 22(3).").

121. GDPR, supra note 13, art. 15 (access) & art. 16 (correction).

122. Emre Bayamlıoğlu, The Right to Contest Automated Decisions Under the General Data Protection Regulation: Beyond the So-Called "Right to Explanation", Regul. & Governance, Mar. 2021, at 1, 5 [hereinafter Bayamlıoğlu, Beyond the So-Called "Right to Explanation"] (explaining that the rights are usually treated as though they are on equal footing as alternatives, without clarity regarding whether they are "complementary, gradual, or distinct rights, or they should be treated as a unity").

123. Id. at 5; Kaminski, Binary Governance, supra note 12, at 1592 (characterizing Article 22 as establishing a version of algorithmic due process).

124. Bayamlıoğlu, Beyond the So-Called "Right to Explanation", supra note 122, at 6.

125. Id.

126. Guidelines on Automated Individual Decision-Making, supra note 115, at 27 (providing that an individual "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").

127. See Andrew D. Selbst & Julia Powles, Meaningful Information and the Right to Explanation, 7 Int'l Data Priv. L. 233, 235 (2017) ("When an individual is subject to 'a deci-

a right to an explanation of automated decisions.[128] While Article 22 is by its nature procedural and not substantive,[129] the existence of an underlying right to contest gives substance to its transparency requirements.[130] That is, according to regulators' guidance, the "right to explanation" of an automated decision requires processors to disclose at least enough information to affected individuals to make contestation actionable.[131] The GDPR's individualized algorithmic transparency requirements are "not about informing or disclosing but rendering the decision contestable at least against a human arbiter."[132]

The right to contestation, like other aspects of the GDPR, in effect obligates companies to both comprehend and to disclose, in the words of Mireille Hildebrandt, "the justification of such decision-making rather than its explanation in the sense of its heuristics."[133] For complex machine-learning systems, this may be challenging if not impossible. It will require creative thinking about how to build such systems so they are not just "explainable" in terms of counterfactuals, but "justifiable" in terms of understanding, revealing, and making challengeable the normative grounds of a decision.

The right to contestation is thus strangely both central to the GDPR's system of algorithmic accountability and barely articulated. Despite its centrality to the GDPR's Article 22, it is not spelled out in the text. Nor does it receive much coverage in the Guidelines issued by the central EU data privacy regulator (the European Data Protection Board) or in the Recitals (the nonbinding preambulatory text accompanying the GDPR).[134] Recital 71 simply and redundantly characterizes the right to contest as a right to "challenge" a decision.[135] The Guidelines largely parrot the text of the

---

sion based solely on automated processing' that 'produces legal effects . . . or similarly significantly affects him or her,' the GDPR creates rights to 'meaningful information about the logic involved.'" (quoting GDPR, supra note 13, art. 22(1))).

128. Kaminski, Right to Explanation, Explained, supra note 25, at 204 ("[A]n 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.").

129. Bayamlıoğlu, Beyond the So-Called "Right to Explanation", supra note 122, at 5–6 ("Due to its procedural character, Article 22/3 is inevitably silent on the substantial grounds which could be relied upon to challenge the reasoning or the criteria underlying the automated decisions . . . whether or when certain [machine-learning] outcome[s] could be regarded as unfair or unlawful is a conclusion . . . [requiring] . . . normative propositions . . . .").

130. Id. at 6 ("In principle, the data controller has to 'explain' the decision in such a way that enables the data subject to assess whether the reasons that led to a particular outcome were legitimate and lawful.").

131. Kaminski, Right to Explanation, Explained, supra note 25, at 204–05.

132. Bayamlıoğlu, Beyond the So-Called "Right to Explanation", supra note 122, at 6.

133. Hildebrandt, Privacy as Protection of the Incomputable Self, supra note 26, at 113.

134. For an explanation of the difference between GDPR text, Recitals, and Guidelines, see Kaminski, Right to Explanation, Explained, supra note 25, at 193–95.

135. See GDPR, supra note 13, Recital 71 (advocating for individuals' right to "obtain human intervention," receive "an explanation of the decision," and "to challenge the decision").

GDPR, and appear in places to conflate contestation with the parallel rights to human intervention and to express one's view.[136]

There has previously been little academic attention to the GDPR's right to contest, and effectively none by U.S. scholars.[137] At one level, this is surprising. The GDPR is one of the first regulatory regimes in the world to regulate AI decision-making, and the right to contestation appears central to its approach, arguably at the core of the individual rights envisioned by the GDPR.[138]

At another level, the lack of attention is understandable. The GDPR is complex and challenging for a U.S. audience to understand.[139] The right to contest may yet be a "paper tiger"—existing on paper but limited in practice.[140] There is little information, even now several years after the GDPR went into effect, about what the right to contestation looks like.[141] The GDPR's contestation rights arise only for "solely automated" decisions with significant effects.[142] And, as is generally the case with individual due process measures, the right to contestation is deeply, and sometimes confusingly, intertwined with other due process measures, especially the more-discussed transparency and notice rights that give it effect.

As section III.B discusses below, the GDPR's right to contestation exists largely for now as a standard, rather than a set of specific procedural rules.[143] Companies must allow individuals to challenge certain automated decisions, but there are as of yet few details about what that process must

136. Guidelines on Automated Individual Decision-Making, supra note 115, at 27, 32.

137. But see Huq, A Right to a Human Decision, supra note 8, at 620–24 (discussing Article 22 as an example of a "right to a human decision," but forgoing deep analysis of its requirements).

138. The regulators that interpret the GDPR have explained that the GDPR's much-debated algorithmic transparency provisions (the "right to explanation") are in service of a more central right to contestation. Guidelines on Automated Individual Decision-Making, supra note 115, at 27. These regulators explain that individuals need a right to explanation in order to be able to contest automated decisions. See Bayamlıoğlu, Contesting Automated Decisions, supra note 27, at 2 ("[T]he right to contest is regarded as the backbone provision with a key role in determining the scope of algorithmic transparency under the GDPR."). But see 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, 6 (2017) (claiming that these rights all could be meaningless).

139. See Meg Leta Jones & Margot E. Kaminski, An American's Guide to the GDPR, 98 Denv. L. Rev. 93, 106–11 (2020) (discussing common errors U.S. readers make when trying to understand the GDPR).

140. Bygrave, Minding the Machine, supra note 10, at 21.

141. Raphaël Gellert, Marvin van Bekkum & Frederik Zuiderveen Borgesius, The Ola & Uber Judgments: For the First Time a Court Recognises a GDPR Right to an Explanation for Algorithmic Decision-Making, EU L. Analysis (Apr. 28, 2021), http://eulawanalysis.blogspot.com/2021/04/the-ola-uber-judgments-for-first-time.html [https://perma.cc/7KP3-2JFV] ("This is the first time that a court in the Netherlands recognises such a right . . . . [I]t is also the first time that a Court anywhere in Europe recognises such a right.").

142. See Kaminski, Right to Explanation, Explained, supra note 25, at 197, 207.

143. See generally Louis Kaplow, Rules Versus Standards: An Economic Analysis, 42 Duke L.J. 557 (1992).

be. This leaves companies, regulators, EU Member States, and eventually courts with a fairly blank (but not entirely blank) slate for implementing the right.

C. *The Right to Contestation Beyond the GDPR*

Despite the nascent state of the GDPR's right to contest, other institutions beyond the EU have already picked up on its importance to algorithmic accountability. The Council of Europe is an international organization, distinct from the EU, that was founded in 1949.[144] At its core is a human rights system, comprising the 1953 European Convention on Human Rights, which is interpreted by the European Court of Human Rights. In April 2020, the Council of Europe adopted a recommendation setting out guidelines to address the human rights impacts of algorithmic systems. It included the guideline to provide "effective *means to contest* relevant determinations and decisions."[145]

The right to contest has also begun to appear in contexts beyond Europe. The 2020 Recommendation of the OECD Council on AI includes a recommendation that users of AI should "enable those adversely affected by an AI system *to challenge its outcome* based on plain and easy-to-understand information on the factors, and the logic that served as the basis for the prediction, recommendation or decision."[146] The OECD recommendations may influence lawmaking and practices in countries around the world.

Individual countries have already adopted or are considering adopting the right to contest. As noted above, Brazil adopted the right in 2018.[147] In November 2020, the Office of the Privacy Commissioner of Canada recommended that Canada revise its data privacy law to afford a right to contest automated decisions.[148] Reasoning that AI decision-making "introduces unique risks that warrant distinct treatment in the

144. Jones & Kaminski, supra note 139, at 101. Note that all EU Member States are parties to the Council of Europe. See Our Member States, Council of Eur., https://www.coe.int/en/web/about-us/our-member-states [https://perma.cc/72W5-ZSGT] (last visited Sept. 7, 2021).

145. Council of Eur., Recommendation CM/Rec (2020) of the Committee of Ministers to Member States on the Human Rights Impacts of Algorithmic Systems 9, 13 (Apr. 8, 2020), https://rm.coe.int/09000016809e1154 [https://perma.cc/2MMJ-WVVC].

146. OECD, Recommendation of the Council on Artificial Intelligence, § 1.3.iv, at 8, OECD Legal Instruments (May 22, 2019), https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449 [https://perma.cc/6KCV-BL2R].

147. LGPD, Art. 20, Law No. 13,709 (Aug. 18, 2018), https://lgpd-brazil.info/chapter_03/article_20 [https://perma.cc/W2CL-SFTW] (Braz.).

148. A Regulatory Framework for AI: Recommendations for PIPEDA Reform, Off. of the Priv. Comm'r of Can. (Nov. 12, 2020), https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-ai/reg-fw_202011/ [https://perma.cc/E6ZL-AP7H].

law," the Commissioner recommended establishing two specific individual rights: a right to explanation and a right to contest.[149]

The Commissioner called for the right to contest to be similar to the GDPR, but explicitly rejected including qualifiers like "solely" in order to ensure that the right applies when automated decisions include more human involvement.[150] The right to contest would, per the Commissioner's Recommendations, entail the ability to "express [one's] point of view to a human intervener, and contest the decision." The Commissioner distinguished between the right to contest and the already existing right to object to data processing, since "contestation provides individuals with recourse even when they choose to continue to participate in the activity for which automated decision-making was employed."[151]

Yet in the United States, proposed and enacted laws fail to include a right to contest AI decisions. The proposed federal Algorithmic Accountability Act of 2019 aimed to create risk assessments for AI systems but did not establish individual rights.[152] A proposed law in Washington State, too, focused on risk assessments and did not establish a right to contest.[153] The newly enacted California Privacy Rights Act, the first in the country to address AI decision-making writ large, tasks the new California Privacy Protection Agency with establishing through regulations a right to opt out of certain kinds of automated decision-making, accompanied by a right to access "meaningful information" about the decision-making process.[154] It does not, however, explicitly describe a right to contest.

One can argue that a number of technology-neutral laws effectively establish a right to contest AI decisions in the United States in certain policy contexts. Litigants have already successfully used due process and administrative procedure claims to challenge government use of AI.[155]

---

149. Id.; see also Cofone, supra note 23.

150. A Regulatory Framework for AI: Recommendations for PIPEDA Reform, supra note 148 ("Unlike the GDPR or Quebec's Bill 64, the term should drop any qualifier such as 'solely' or 'exclusively', which scopes the applicability of specific protections very narrowly. These also make the term susceptible to subversion where a human role is added in the process to merely evade additional obligations.").

151. Id.

152. See, e.g., Algorithmic Accountability Act, S. 1108, 116th Cong. §§ 2–3 (2019).

153. H.B. 1655, 66th Leg., 2019 Reg. Sess. (Wash. 2019) (attempting to establish "algorithmic accountability reports"). Additionally, the latest proposed Washington Privacy Act mimics the GDPR in calling for data impact assessments but fails to establish an individual right to contest automated decisions. See S.B. 5062, 67th Leg., 2021 Reg. Sess. (Wash. 2021).

154. Cal. Civ. Code § 1798.185(16) (2021).

155. Huq, Constitutional Rights in the Machine-Learning State, supra note 8, at 1895–98 (citing successful due process claims against the government's use of machine-learning algorithms for significant decisions); see also Rashida Richardson, Jason M. Schultz & Vincent M. Southerland, AI Now Inst., Litigating Algorithms 2019 US Report: New Challenges to Government Use of Algorithmic Decision Systems 28–32 (2019), https://ainowinstitute.org/litigatingalgorithms-2019-us.html [https://perma.cc/MJF4-3T3E].

Antidiscrimination law, too, might in some circumstances be used to challenge decisions made using AI.[156] Existing doctrines, however, present hurdles in the AI context, not the least of which is evidentiary.[157] There are benefits to a clearly established and cross-contextual right to contest AI.

D. *Academic Views on Regulating AI*

Academic views on regulating AI can both illustrate and influence policymakers' thinking on whether to establish a right to contest AI. There is a fast-growing literature considering how to regulate complex computer algorithms. Yet while earlier scholars called for some kind of due process, the recent trend has been to favor systemic governance over the companies or government entities that build and use AI over establishing individual rights such as a right to contest.[158]

A first wave of scholars on algorithmic accountability called for "technological due process" or "big data . . . due process."[159] In *Technological*

---

156. Plaintiffs do face an "uphill battle," both for disparate impact claims generally and with regards to big data inferences in particular. See Ajunwa, Auditing Imperative, supra note 4, at 647 ("[P]laintiffs aiming to bring an employment discrimination claim on a theory of disparate impact, rather than disparate treatment, face an uphill battle."); Barocas & Selbst, Big Data's Disparate Impact, supra note 70, at 674 ("[A]ttempts to certify the absence of prejudice on the part of those involved in the data mining process may wrongly confer the imprimatur of impartiality on the resulting decisions."). Ajunwa has instead proposed a third cause of action under Title VII of "discrimination per se" whereby:

> [A] plaintiff [could] assert that a hiring practice (for example, the use of proxy variables [in automated hiring] resulting or *with the potential to result in* adverse impact to protected categories) is so egregious as to amount to *discrimination per se*, and this would shift the burden of proof from the plaintiff to the defendant (employer) to show that its practice is nondiscriminatory.

Ajunwa, Paradox of Automation, supra note 4, at 1728.

157. Huq, Constitutional Rights in the Machine-Learning State, supra note 8, at 1897 ("I have not been able to find examples of challenges to algorithmic allocation systems based on equality or privacy concerns. This may be because due process claims are easier to allege."); see also Barocas & Selbst, Big Data's Disparate Impact, supra note 70, at 694–714 (describing challenges for Title VII claims about machine-learning algorithms).

158. Kaminski, Binary Governance, supra note 12, at 1540 n.34; see also Huq, Constitutional Rights in the Machine-Learning State, supra note 8, at 1550 ("Those scholars who reject individualized algorithmic due process and individualized transparency largely implicitly reject both the dignitary and justificatory rationales for them. They understand regulating private-sector algorithms as being largely about correcting error or discrimination and bias."); id. at 1557 ("A growing body of literature calls for moving away from ex post, individualized transparency and due process or, at least, supplementing them with regulations that target algorithmic design at earlier stages and target the human systems around algorithms.").

159. Citron, Technological Due Process, supra note 3, at 1301; Citron & Pasquale, Scored Society, supra note 8, at 27; Crawford & Schultz, supra note 8, at 124; see also Maayan Perel & Niva Elkin-Koren, Accountability in Algorithmic Copyright Enforcement, 19 Stan. Tech. L. Rev. 473, 496 (2016) ("Affected individuals should have the rights to inspect, correct, and dispute what they believe to be inaccurate adjudication decisions made with respect to their online conduct."); Schwartz, supra note 61, at 1343–74; Daniel J. Steinbock,

Due Process, Danielle Citron observed the increasing governmental use of computer algorithms for decision-making.[160] Citron called for systemic regulation, drawing on the Administrative Procedure Act as both a model and a legal constraint, and for individualized due process. She noted, however, that *Mathews v. Eldridge* could present hurdles to individual challenges in practice because of the potential expense involved in challenging algorithmic systems.[161]

Several years later, two sets of scholars called for extending "due process"-like protections to private sector decisions.[162] Kate Crawford and Jason Schultz drew heavily on due process theory—drawing on the work of Martin Redish and Lawrence Marshall,[163] and Judge Henry Friendly[164]—to build an argument for individualized process in the face of predictive data analytics.[165] In *The Scored Society: Due Process for Automated Predictions*, Citron and Frank Pasquale similarly explained that "[p]rocedural protections should apply not only to the scoring algorithms themselves (a kind of technology-driven rulemaking), but also to individual decisions based on algorithmic predictions (technology-driven adjudication)."[166] These scholars called for systemic regulatory oversight, but not to the exclusion of process protections (or rights) for individuals.

These pathbreaking works, however, do not provide much guidance for implementing an individual right to contest automated decisions. Citron suggested that government decision-makers could be required to explain their use of an automated system's decision and should be educated about such systems' biases, while the systems should be tested for error and bias.[167] Crawford and Schultz called for a "neutral data arbiter" such as the FTC to investigate complaints against private parties "based on predictive privacy harms and, in the process of those complaints, investigate the basis of the predictions."[168] It is not clear whether *every* individual complaint would result in an individualized hearing; this seems unlikely

---

Data Matching, Data Mining, and Due Process, 40 Ga. L. Rev. 1, 64–81 (2005) (addressing government use of data mining in the context of air passenger screening and the creation of watch lists); Zarsky, Transparent Predictions, supra note 9, at 1553–68 (offering an exhaustive analysis of transparency in algorithmic decision-making and calling for procedural protections).

160. Citron, Technological Due Process, supra note 3, at 1259, 1263–67.

161. Id. at 1284–85.

162. Citron & Pasquale, Scored Society, supra note 8; Crawford & Schultz, supra note 8.

163. See Martin H. Redish & Lawrence C. Marshall, Adjudicatory Independence and the Values of Procedural Due Process, 95 Yale L.J. 455, 474 (1986) (describing the need for "a model of procedural due process that simultaneously allows the flexibility central to the due process concept as it has evolved, while providing a principled and workable structure").

164. See Friendly, supra note 2, at 1268–1304.

165. Crawford & Schultz, supra note 8, at 114–20.

166. Citron & Pasquale, Scored Society, supra note 8, at 19.

167. Citron, Technological Due Process, supra note 3, at 1304–11.

168. Crawford & Schultz, supra note 8, at 127.

given the limited capacities of the FTC.[169] Citron and Pasquale called, too, for regulatory oversight by the FTC.[170] They also called for individualized notice guaranteed by audit trails,[171] and interactive modeling to let individuals better understand the scoring algorithms used against them.[172] While they referred to "challenge[s]" against algorithmic scoring, they did not go into detail about what such an "opportunity to be heard" might constitute in practice.[173]

In any event, despite this initial enthusiasm for individual due process, more recent proposals have largely shied away from it. Some scholars have simply ignored individual due process and related transparency rights; others have explicitly rejected them. In *Accountable Algorithms*, a bevy of interdisciplinary authors listed potential harms of transparency—obviating the "notice" portion of individual due process rights.[174] Other scholars have critiqued individual rights as ineffective fallacies, citing a lack of individual capacity and access to justice issues.[175] Several scholars have noted that due process applies only in the context of state action.[176]

Aziz Huq has gone further, arguing that due process rights should not apply even to state action—or rather, that instead of individualized challenges to algorithmic decision-making, individuals should be able to challenge whether the algorithm is systemically "well-calibrated."[177]

There are limited exceptions to the trend. Rory Van Loo, for example, calls for a complex appeals system to apply to platform decision-making, involving transparent precedent established by neutral human arbiters.[178] In the criminal trial context, Andrea Roth calls for a confrontation right with respect to machine-created evidence, including tools ranging from

---

169. Crawford and Schultz seem more concerned about obtaining transparency and checking bias at the level of the general public. Id. at 127 ("The presence of a neutral data arbiter would provide the public with an opportunity to be heard, to examine the evidence used in adjudicative predictions, and to challenge it.").

170. Citron & Pasquale, Scored Society, supra note 8, at 20–27.

171. Id. at 28.

172. Id. at 28–29.

173. Id. at 27–28, 33.

174. See Joshua A. Kroll, Joanna Huey, Solon Barocas, Edward W. Felten, Joel R. Reidenberg, David G. Robinson & Harlan Yu, Accountable Algorithms, 165 U. Pa. L. Rev. 633, 657–60 (2017).

175. See, e.g., 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. 18, 74–75 (2017).

176. See, e.g., Deven R. Desai & Joshua A. Kroll, Trust but Verify: A Guide to Algorithms and the Law, 31 Harv. J.L. & Tech. 1, 43, 46 (2017) ("Although due process concerns explain why we would require the creation of robust trails of evidence for software-driven decision processes in government, whether the same is true for private sector uses turns on the nature of the private activity at issue.").

177. Huq, A Right to a Human Decision, supra note 8, at 686; Huq, Constitutional Rights in the Machine-Learning State, supra note 8, at 1909–10.

178. Van Loo, supra note 5, at 867–78.

courtroom testing to cross-examination of responsible programmers.[179] These arguments, however, are site specific, and do not call for a general right to contest AI.

We turn, then, to the limited academic literature on the legal right most analogous to what we propose: the GDPR's right to contest an automated decision. The GDPR's right to contestation has received surprisingly little scholarly attention. Instead, much ink has been spilled over the related "right to explanation" of an algorithmic decision.[180] There, again, we see considerable backlash against an individualized transparency right.[181] Even in Europe, where there is a relatively robust conception of data privacy as a human right that contributes to protecting individual dignity, much of the literature has focused on the efficacy of systemic oversight, rather than the individual rights the GDPR has to offer.[182] One of the only European scholars to examine the GDPR's right to contestation, Emre Bayamlıoğlu, does argue that contestation is a necessity and "requires a mechanism which will enable data subjects to have their objection heard in a process intelligible to them—with the possibility of an outcome for the annulment or the amendment of the decision."[183] By contrast, Huq, who is one of the only U.S. scholars to directly address the GDPR's right to contestation, explicitly rejects it in favor of a "right to a well-calibrated machine decision"—that is, a right not to an individual challenge, but to a systemically well-functioning machine.[184]

Instead of an individualized right to contest, scholars recently have proposed systemic measures that regulate the companies or government agencies that build or use the AI. These measures include: ex ante testing, design requirements, impact assessments, recording requirements that document how an algorithm was trained and what data was chosen to train it, whistleblower protections, and creation of a public interest cause of action.[185]

---

179. Roth, supra note 79, at 2050 (suggesting the use of programmer testimony before an expert panel, written interrogatories to programmers, access to source code, and the disclosure of prior statements of machines).

180. Kaminski, Right to Explanation, Explained, supra note 25, at 192 n.8.

181. See, e.g., Edwards & Veale, supra note 175, at 74–75; Wachter et al., Why a Right to Explanation of Automated Decision-Making Does Not Exist, supra note 111.

182. See, e.g., Edwards & Veale, supra note 175, at 74. On the EU and dignity, see Jones, The Right to a Human in the Loop, supra note 72, at 231; Tal Z. Zarsky, Incompatible: The GDPR in the Age of Big Data, 47 Seton Hall L. Rev. 995, 1016–17 (2017) [hereinafter Zarsky, Incompatible].

183. Bayamlıoğlu, Transparency of Automated Decisions, supra note 9, at 39.

184. Huq, A Right to a Human Decision, supra note 8, at 686.

185. See Desai & Kroll, supra note 176, at 43 ("We begin this Part by looking at public sector decision-making and explain why technical accountability is necessary as a matter of due process . . . we [also] offer a possible statutory change—the passage of law to encourage and protect whistleblowers who know of prohibited practices."); Huq, Constitutional Rights in the Machine-Learning State, supra note 8, at 1940 ("Aggregate challenges (such as class actions, facial challenges, and the like) usefully direct attention to system-wide causes of

These systemic governance proposals have value. Systemic governance is likely necessary for governing AI, given the very real challenges individuals face in contesting such systems.[186] An individual right to contest by itself would likely fail to fully address or mitigate harms. Because of the nature of the technology and the locus of expertise in the private sector, AI, too, may be particularly well suited to innovative "new governance" or "collaborative governance" models that harness the strengths of both government and industry.[187]

But current scholarship leaves largely unsettled the question of whether there also is value in subjecting algorithmic decision-making to contestation. Consequently, it also fails to address how to design and implement an effective contestation right.

II. WHY HAVE A RIGHT TO CONTEST AI?

This Part takes a deeper look at the theory underpinning the Western tradition of individual due process and considers whether it provides purchase for an individual right to contest AI decisions.

---

constitutional harm."); Sonia K. Katyal, Private Accountability in the Age of Artificial Intelligence, 66 UCLA L. Rev. 54, 115–17, 126–29 (2019) (encouraging a thorough examination ex ante and ex post of the algorithm and the training data employed to refine the algorithm); Selbst, Disparate Impact in Big Data Policing, supra note 59, at 169–72 (discussing the possibility of an Algorithmic Impact Statement requirement in the model of Environmental Impact Statements); Andrew D. Selbst & Solon Barocas, The Intuitive Appeal of Explainable Machines, 87 Fordham L. Rev. 1085, 1100–05, 1110–17 (2018) [hereinafter Selbst & Barocas, Intuitive Appeal] (discussing how the techniques available within machine learning for ensuring interpretability correspond well to the different types of explanation required by existing law); Andrew D. Selbst, An Institutional View Of Algorithmic Impact Assessments, 35 Harvard J.L. & Tech. (forthcoming 2021) (UCLA Sch. of Law, Public Law Research Paper No. 21–25) (manuscript at 4–5), https://ssrn.com/abstract=3867634 [https://perma.cc/667V-3XAG] (discussing the goals and potential efficacy of [algorithmic impact assessments] and arguing that the regime requires good-faith participation by the private sector).

186. Kaminski, Binary Governance, supra note 12, at 1557 ("While individual rights can address important dignitary and justificatory concerns, there are better ways to identify and fix systemic problems in algorithmic decision-making.").

187. Id. at 1559–77 (discussing the promises and pitfalls of collaborative governance of algorithms, including a lack of accountability and enforcement mechanisms); Michael Guihot, Anne F. Matthew & Nicolas P. Suzor, Nudging Robots: Innovative Solutions to Regulate Artificial Intelligence, 20 Vand. J. Ent. & Tech. L. 385, 427, 441, 445 (2017) (calling for a mix of self-regulation and risk regulation in the form of soft-law, regulatory "nudge[s]"); Perel & Elkin-Koren, supra note 159, at 529–31 ("We advocate a collaborative-dynamic regulation . . . ."); Alicia Solow-Niederman, Administering Artificial Intelligence, 93 S. Cal. L. Rev. 633, 640, 645 (2020). On collaborative governance generally, see Orly Lobel, New Governance as Regulatory Governance, *in* The Oxford Handbook of Governance 65, 66–67 (David Levi-Faur ed., 2012); Jody Freeman, Collaborative Governance in the Administrative State, 45 UCLA L. Rev. 1, 21–33 (1997); Orly Lobel, The Renew Deal: The Fall of Regulation and the Rise of Governance in Contemporary Legal Thought, 89 Minn. L. Rev. 342, 371–76 (2004).

As discussed above, contestation is an ancient concept that remains core to the Western tradition of justice.[188] In the U.S. legal system, contestation rights most prominently extend from the Due Process Clause of the Fifth Amendment.[189] Contrary to what some may believe, however, in the United States, contestation is not limited to government decisions. Layers of positive law developed in specific policy contexts afford individuals procedural protections, including rights to access and correct personal information[190] and rights to contest credit card charges.[191] Understanding that U.S. law already imposes rights to contest the decisions of private companies is important context for any discussion of a right to contest AI, as private companies' algorithms can make decisions as significant as any government body's.[192]

Contestation rights do not always provide justice. Contestation may occur ex post, when some harms cannot be undone or ameliorated. Contestation may be too slow. It may be too costly.[193] Information, power, and influence asymmetries between the disputants may tilt the process toward unfairness. A right to contest may be neither sufficient to protect fundamental rights nor self-executing.

But while a right to contestation may not be sufficient to protect fundamental rights, it may yet be necessary. The next section discusses the reasons frequently given for establishing individual process rights and notes their resonance with recent discussions of rights to contest AI decisions.

A. *Why Have Due Process?*

As discussed above, a few scholars have called for establishing individual due process for algorithmic decision-making, drawing on several core

188. See supra notes 88–91 and accompanying text.

189. Rules of evidence, too, can be understood as an important aspect of contestation, mandating disclosure or limiting the use of particular pieces of information in legal challenges. See, e.g., Roth, supra note 79, at 2039–51; Wexler, supra note 6, at 1395–429.

190. See California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100–1798.199.100; California Privacy Rights Act of 2020, Proposition 24 (2020) (to be codified at Cal. Civ. Code §§ 1798.100–1798.199.100); Virginia Consumer Data Protection Act, 2021 Va. Special Sess. Law I, ch. 52 (2021) (to be codified at Va. Code Ann. §§ 59.1-571–59.1-581 (2023)).

191. Van Loo, supra note 5, at 851.

192. See, e.g., Citron & Pasquale, Scored Society, supra note 8, at 8–13 (discussing credit scoring and other algorithmic ranking systems); Van Loo, supra note 5, at 836–50 (discussing decisions made by technology platforms about speech, lodging, commerce, elections, and reputation).

193. Procedural safeguards that are too costly may not be required. See, e.g., Mathews v. Eldridge, 424 U.S. 319, 333–35 (1976) (providing for a cost-benefit analysis to decide which specific safeguards will be required as part of an "opportunity to be heard"). In *Technological Due Process*, Citron observes that *Mathews* likely poses a challenge to requiring expert analysis of automated decisions, though she argues that the cost of an expert to correct the computer logic in one case of erroneous automated decision-making should be weighed against the benefits the correction provides for all future cases. Citron, Technological Due Process, supra note 3, at 1284–86.

texts of due process theory.[194] Further exploration of the due process literature sheds additional light on the role of a right to contest.

The Due Process Clause of the Fifth Amendment requires that "[n]o person shall . . . be deprived of life, liberty, or property, without due process of law."[195] In practice this requires notice and an opportunity to be heard "appropriate to the nature of the case."[196] But why? The rationales for due process include obtaining accuracy, supporting rule of law values, and liberal theory—that is, theory that emphasizes the importance of the individual who is affected by a given decision.

1. *Accuracy.* — A common answer to the question of why we have due process is an instrumentalist one: to ensure accuracy.[197] The Supreme Court has stated more than once that "[t]he function of legal process . . . is to minimize the risk of erroneous decisions."[198] Accuracy is commonly named as a reason for robust contestation mechanisms.[199] This is ancient reasoning: The Bible cautions that "[t]he one who first states a case seems right, until the other comes and cross-examines."[200] This reasoning also retains force today. For example, only individual administrative appeals and lawsuits revealed the problems with the home-health-care allocation algorithm discussed above.[201]

But our legal system does not even in the highest-stakes contexts guarantee individuals an accurate decision.[202] Rather, accuracy is often treated as a goal or value to be balanced against other goals or values, such as cost and efficiency.[203] Some scholars have thus taken accuracy to be a systematic

194. See, e.g., Citron, Technological Due Process, supra note 3, at 1258; Cary Coglianese & David Lehr, Transparency and Algorithmic Governance, 71 Admin. L. Rev. 1, 40–43 (2019); Crawford & Schultz, supra note 8, at 127.

195. U.S. Const. amend. V.

196. Cleveland Bd. of Educ. v. Loudermill, 470 U.S. 532, 542 (1985) (quoting Mullane v. Cent. Hanover Bank & Tr. Co., 339 U.S. 306, 313 (1950)).

197. See Huq, A Right to a Human Decision, supra note 8, at 653; Redish & Marshall, supra note 163, at 476–81 (naming accuracy as one of seven values protected by procedural due process).

198. Greenholtz v. Inmates of the Neb. Penal & Corr. Complex, 442 U.S. 1, 13 (1989); Huq, A Right to a Human Decision, supra note 8, at 653 n.201 (citing Heller v. Doe ex rel. Doe, 509 U.S. 312, 332 (1993)); see also Jerry L. Mashaw, The Supreme Court's Due Process Calculus for Administrative Adjudication in *Mathews v. Eldridge*: Three Factors in Search of a Theory of Value, 44 U. Chi. L. Rev. 28, 48 (1976) ("The *Eldridge* Court . . . views the sole purpose of procedural protections as enhancing accuracy . . . .").

199. See, e.g., Crawford & Schultz, supra note 8, at 126–27 (touting a hearing before a neutral arbiter as a way to preserve fairness, accuracy, and other values); Redish & Marshall, supra note 163, at 476.

200. Proverbs 18:17 (NSRV).

201. See Lecher, supra note 80; McCormick, supra note 56.

202. Huq, A Right to a Human Decision, supra note 8, at 653 ("But even in high-stakes contexts such as criminal cases or post-conviction review of capital punishment, the Supreme Court has shied away from a personal right to a *true* determination.").

203. See Crawford & Schultz, supra note 8, at 115; Friendly, supra note 2, at 1276 ("[A]t some point, the benefit to individuals from an additional safeguard is substantially out-weighed by the cost of providing such protection . . . .").

management goal, meaning that to the extent individual due process can in the aggregate make a decisional system more accurate, it is worth protecting.[204] If this were the only reason for protecting individual process, however, individual process would not be worth protecting to the extent it failed to make a decisional system more accurate. Accuracy thus may be a central goal of individual process, but it alone cannot account for strong intuitions people have about what is just or fair.

2. *Rule of Law Values.* — A second reason to establish individual rights to contest is to respect rule of law values. These values suggest that a decisional system should be fair, consistent, predictable, and rational across different individuals.[205] Allowing individuals to contest decisions reveals whether a decisional system is unfair, inconsistent, arbitrary, unpredictable, or irrational. Contestation and its accompanying procedural protections, such as reason giving, require that a decision-maker demonstrate examinable commitment to an outcome and describe the reasons for it.[206] This aims to prevent arbitrariness and allow for quality control of decisions, including sniffing out bias or discrimination.[207] That is, contestation might help eliminate the pitfalls of decisional discretion, while leaving decision-makers the ability to tailor rules to individual circumstances.

But again, the rule of law rationale could be characterized as arguing for individual protections from an underlying focus on the decisional system as a whole. The central concern with the rule of law rationale is over the legitimacy of the system of decision-making, not necessarily the individuals within it. Thus, rule of law reasoning might leave space, like the accuracy rationale, for arguments that individual rights to contest are necessary only to the extent that they reveal unfairness, arbitrariness, unpredictability, and irrationality. Indeed, we see echoes of this reasoning in the literature on algorithmic accountability, with scholars rejecting individual rights in favor of other measures that in their view are adequate for ensuring that a decisional system as a whole is not arbitrary or irrational.[208]

3. *Liberal Theory.* — To fully consider the potential value of an individual right to contest, we need theory that is grounded in individuals. This

204. See Crawford & Schultz, supra note 8, at 121; Jerry L. Mashaw, The Management Side of Due Process: Some Theoretical and Litigation Notes on the Assurance of Accuracy, Fairness, and Timeliness in the Adjudication of Social Welfare Claims, 59 Cornell L. Rev. 772, 815–16 (1974) (asserting that due process requires greater protection for the claimant and should include the application of systematic management).

205. See Crawford & Schultz, supra note 8, at 119 (citing Redish & Marshall, supra note 162, at 483–86).

206. Frederick Schauer, Giving Reasons, 47 Stan. L. Rev. 633, 649 (1995) [hereinafter Schauer, Giving Reasons].

207. See id. at 657 ("But when institutional designers have grounds for believing that decisions will systematically be the product of bias, self-interest, insufficient reflection, or simply excess haste, requiring decisionmakers to give reasons may counteract some of these tendencies.").

208. See Kroll et al., supra note 174, at 662–72 (discussing computational methods that can provide accountability for procedural regularity while balancing privacy concerns).

section turns to what Jerry Mashaw terms "the liberal tradition" in U.S. constitutional theory, which "has at its core the notion that individuals are the basic unit of moral and political value."[209] Mashaw has argued, convincingly, that there is a long tradition of at least three categories of liberal theory that could be behind calls for individual due process: Benthamite (utilitarian), Lockean (natural rights), and Kantian (personhood) theories.[210] This section examines each in turn.

At first glance, utilitarianism might seem an ill fit for an argument that individual rights matter. Utilitarianism, after all, is primarily concerned with maximizing outcomes for society as a whole.[211] There are, however, three ways in which utilitarianism can support an individual right to contest.[212] First, utilitarians might argue through classic cost-benefit analysis that individual process produces acceptance or even happiness on the part of affected individuals, which makes it more likely that the decisional system as a whole will achieve social welfare goals. Second, utilitarians sometimes (albeit rarely) argue for individual rights based on the idea that certain protections are so likely to be correct in terms of social welfare maximization that it makes sense to establish those protections as default rules ("rule utilitarianism").[213] Under rule utilitarianism, society should establish individual process as a rule when it is more likely to maximize social welfare—if it prevents pain or other seriously negative consequences.[214] Finally, utilitarians do recognize the existence of a private sphere for individuals in which social welfare calculations have no place.[215] If a decisional system threatens to impinge on that private sphere, individual process rights arguably should apply.

From a Lockean or natural rights perspective, individual due process is understood as a means of protecting underlying natural entitlements. Lockean analysis centers around the idea of the "natural rights" inherent in individuals, such as the rights to life, liberty, and property.[216] If the government reallocates or significantly impinges upon these rights, it must do so through adequate process. The goal of process under a Lockean analysis is to (1) avoid errors, or if that is not possible, (2) indicate "consent" to

209. Jerry L. Mashaw, Administrative Due Process: The Quest for a Dignitary Theory, 61 B.U. L. Rev. 885, 907 (1981) [hereinafter Mashaw, Administrative Due Process] (emphasis added).

210. Id.

211. Id. at 910.

212. Id.

213. Id. at 911.

214. Id.

215. Id. (referencing the work of John Stuart Mill in noting that "the approach [of separating the individual and the social] does yield at least a dignitary process restraint—some notion of individual privacy that is beyond social invasion because it is necessary to social welfare").

216. Id. at 908–09 (discussing the work of John Locke and Robert Nozick).

such reallocations or impingements by the affected individuals.[217] Thus in circumstances where natural rights are affected, process is intended to help mitigate error, and evidences individual buy-in (if not consent). The limit to the Lockean argument for due process is that process is tied to protection of these certain core substantive rights; it is not justified in and of itself.

Finally, we turn to Kantian or dignitary theory. Current scholarship on algorithmic accountability largely ignores or rejects the dignitary tradition in U.S. thought.[218] More broadly, privacy scholarship for the most part concedes that while Europe is concerned about dignity, the United States is not.[219] This overstates the case. Examining due process theory shows that there is a long dignitary tradition in the United States, and we overlook it to our detriment.

The Kantian categorical imperative is that individuals must be treated as an end in themselves, not as the means to an end.[220] A right to contest significant decisions is an expression of this value. The strongest form of a Kantian/dignitary argument for process is that using proxy categories to make decisions about individuals treats them as objects and thus violates their dignity—unless they are afforded opportunities for individualized judgment.[221] One need not subscribe to this strongest form, however, to acknowledge the dignitary argument for due process.

A Kantian approach argues that due process rights are necessary to respect individual selfhood. Opaque or arbitrary decisions fundamentally interfere in such self-respect. Offering a reason for a decision, by contrast,

---

217. Id. at 909.

218. See Huq, A Right to a Human Decision, supra note 8, at 652 (describing dignity as an "ambiguous and contested" concept); Selbst & Barocas, Intuitive Appeal, supra note 185, at 1119 ("To the extent that the personhood rationale can be converted to a more actionable legal issue, it is reflected in the concept of 'procedural justice[]' . . . .").

219. See, e.g., Joel R. Reidenberg, Resolving Conflicting International Data Privacy Rules in Cyberspace, 52 Stan. L. Rev. 1315, 1341–54 (2000) (contrasting the United States' liberal approach to information privacy with Europe's social-protection approach); James Q. Whitman, The Two Western Cultures of Privacy: Dignity Versus Liberty, 113 Yale L.J. 1151, 1180–89 (2004) (describing the philosophical origins of privacy law); see also Jones, The Right to a Human in the Loop, supra note 182, at 217.

220. Immanuel Kant, Foundations of the Metaphysics of Morals: And What is Enlightenment? 47 (Lewis White Beck trans., 1959) (1785) ("Act so that you treat humanity, whether in your own person or in that of another, always as an end and never as a means only."); Edmund L. Pincoffs, Due Process, Fraternity, and a Kantian Injunction, *in* Due Process: NOMOS XVIII 172, 179 (J. Roland Pennock & John W. Chapman eds., 1977) ("[P]articipation is an instrument by which the valuation of persons as ends in themselves is expressed."); Mashaw, Administrative Due Process, supra note 209, at 915 ("The direct application of the Kantian categorical imperative, in which dignity may be said to consist in being treated as an end in oneself rather than as instrumental to the ends of others, may thus yield a robust set of procedural rights.").

221. Mashaw, Administrative Due Process, supra note 209, at 897, 901. According to Mashaw, this "principle has no obvious limits." Id. at 897; see also Kaminski, Binary Governance, supra note 12, at 1541–42.

shows a sign of respect for the decisional subject.[222] So does enabling participation in the legitimacy of the system by establishing a right to contest its outputs. When a decision affects certain fundamental rights, process is necessary as both a means for promoting accuracy with respect to rights deprivation and an end for enabling self-respect.[223]

B. *AI Decisions and Due Process Values*

Centering the individual in the due process inquiry is thus not a foreign concept. The question remains whether AI decision-making, including by private entities, should be subject to a right to contest. This section begins with some history, addressing the influential 1973 HEW Report and its emphasis on due process. It then applies the reasoning above—instrumentalism, rule of law values, and liberal theory—to the question of whether individuals should be afforded due process in the face of significant decision-making by AI.

1. *The HEW Report: Due Process for Data Processing*. — The idea that automated data processing—including by private entities—implicates due process values has deep roots in the United States. In the early 1970s, then-Secretary of Health, Education, and Welfare Elliot L. Richardson established an Advisory Committee on Automated Personal Data systems.[224] In establishing the Committee, Richardson declared that "there is a growing concern that automated personal data systems present a serious potential for harmful consequences, including infringement of basic liberties. This has led to the belief that special safeguards should be developed to protect against potentially harmful consequences for privacy and due process."[225]

In 1973, the Committee published an influential report (the HEW Report),[226] often characterized as a foundational document for data privacy lawmaking. Data privacy laws both in the United States and around the world have since been based on the Report's core principles, though the United States diverged in significant ways from its counterparts abroad.

The HEW Report takes a highly procedural approach to information privacy, with due process principles running throughout. The Report notes that conventionally, privacy is often equated with secrecy or seclusion.[227] That is, shared information is presumed to be no longer private.[228] This conception of privacy is a poor fit, however, for the privacy interests in personal

222. Schauer, Giving Reasons, supra note 207, at 658.

223. Mashaw, Administrative Due Process, supra note 209, at 919–20.

224. HEW Report, supra note 68, at viii.

225. Id.

226. Id. at vi–vii.

227. See id. at 38 ("Dictionary definitions of privacy uniformly speak in terms of seclusion, secrecy, and withdrawal from public view. They all denote a quality that is not inherent in most record-keeping systems.").

228. See Margot E. Kaminski, Regulating Real-World Surveillance, 90 Wash. L. Rev. 1113, 1124 (2015) [hereinafter Kaminski, Regulating Real-World Surveillance] ("Courts

data held and processed as part of a system of record keeping. Individuals often deliberately hand over personal data for limited use, yet still retain some expectation of privacy in them.[229]

The HEW Report thus formulates a conception of data privacy intended to both allow "some *disclosure* of data" and afford affected individuals at least some agency in deciding "the nature and extent of such disclosure."[230] That is, the Report's founding principle is that both the organizations that process records and the individuals affected by such records should be able to participate in constructing what data privacy means in practice.[231] As organizations typically control such decisions with little input by affected individuals, the HEW Report's safeguards (later known as the fair information practice principles or "FIPPs") are largely geared toward providing procedural protections for affected individuals.

The result is a set of procedures and standards rather than substantive determinations. The Report notes that its safeguards do not

> provide the basis for determining *a priori* which data should or may be recorded and used, or why, and when. [They do], however, provide a basis for establishing procedures that *assure the individual a right to participate* in a meaningful way in decisions about what goes into records about him and how that information shall be used.[232]

Like due process, such procedural safeguards include notice[233] and various rights to be heard.[234] As scholars later note, these are the foundations of a kind of due process for data processing.[235]

The HEW Report stands as a counterargument to the idea that only Europeans care about dignity and due process in the context of automation.[236] The Report's reasoning reflects the range of concerns about

---

have tended to rely on a privacy binary: information is either withdrawn and thus private, or available to others and thus public. Once information is shared with others under this rubric, it can no longer be protected as private."); Neil M. Richards & Daniel J. Solove, Prosser's Privacy Law: A Mixed Legacy, 98 Calif. L. Rev. 1887, 1920 (2010) (noting that the all-or-nothing nature of privacy makes it nearly impossible to keep information completely hidden).

229. See Kaminski, Regulating Real-World Surveillance, supra note 228, at 1127 ("[People] choose to reveal information under particular circumstances, expecting that it will not travel beyond those settings.").

230. HEW Report, supra note 68, at 39–40.

231. The HEW Report refers to this as "mutuality." Id. at 40.

232. Id. at 41.

233. See id. ("There must be no personal-data record-keeping systems whose very existence is secret.").

234. See id. ("There must be a way for an individual to correct or amend a record . . . .").

235. See Crawford & Schultz, supra note 8, at 108 (noting that the FIPPS provide "notice, choice, and control to users ex ante any privacy harm" and observing the challenges of doing so for Big Data privacy harms).

236. See generally supra note 218 (questioning or dismissing dignitary concerns as the basis of algorithmic due process and transparency). On the EU and dignity, see Jones, The Right to a Human in the Loop, supra note 72, at 220–24; Zarsky, Incompatible, supra note 182, at 1016–17.

computerized decision-making articulated in this Article: concerns about accuracy, fairness, individualized flexibility, dignity, and dehumanization. The Report observes that data processing can "sacrifice flexibility and accuracy" in the name of efficiency, contributing to the "the so-called 'dehumanizing' image of computerization."[237] It evinces concern about both inaccuracy and unfairness.[238] It identifies the problem of "statistical stereotyping," in which data processing is used to predict an individual's future behavior based on his placement into a "statistically defined group."[239] The way to mitigate problems, the Report notes, is to "permit[] an individual to know that he has been labelled a risk and to *contest* the label as applied to him."[240]

The HEW Report, whose principles now form the backbone of federal U.S. sectoral data privacy laws such as HIPAA and COPPA, is thus as much about due process as it is about what most people would term privacy. It proposes process safeguards to mitigate the power asymmetries between individuals and the organizations, public and private, that hold records on them.[241]

To be clear, there have been many valid critiques of how the United States has since operationalized privacy regulation, outside of the above-named statutory regimes, around a watered-down version of individual control.[242] The dominant U.S. approach to privacy protection has been "notice and choice," in which individuals are expected to "read [privacy] notices and make decisions according to their overall preferences."[243] This approach has been criticized for, among other things, creating a legal fiction of consent when nobody in fact reads privacy policies; overly relying on individuals' time, attention, and expertise; and overlooking the extent to which technology platforms manip-

237. HEW Report, supra note 68, at 14.

238. See id. at 19 ("[T]he likelihood of unfair or inappropriate decisions about the individual to whom any given record pertains will be a problem . . . .").

239. See id. at 26.

240. Id. (emphasis added).

241. See id. at 28–29 ("[A]n individual's control over the personal information that he gives to an organization, or that an organization obtains about him, is lessening as the relationship between the giver and receiver of personal data grows more attenuated, impersonal, and diffused.").

242. See, e.g., Julie E. Cohen, Configuring the Networked Self: Law, Code, and the Play of Everyday Practice 10 (2012) ("The consensus view in U.S. privacy theory tends to be that there is essentially no legitimate expectation of privacy under these circumstances and that the surveillance therefore should not trouble us."); Julie E. Cohen, What Privacy Is For, 126 Harv. L. Rev. 1904, 1927–30 (2013) (noting how the paradigm of "new privacy governance" evolving in the U.S. legal system is rooted in a regulatory ideology that downplays the "need to hold market actors accountable for harms to the public interest"); Daniel J. Solove, Introduction: Privacy Self-Management and the Consent Dilemma, 126 Harv. L. Rev. 1880, 1880–82 (2013) [hereinafter Solove, Privacy Self-Management and the Consent Dilemma] ("Although privacy self-management is certainly a laudable and necessary component of any regulatory regime, I contend that it is being tasked with doing work beyond its capabilities. Privacy self-management does not provide people with meaningful control over their data.").

243. Chris Jay Hoofnagle & Jennifer M. Urban, Alan Westin's Privacy *Homo Economicus*, 49 Wake Forest L. Rev. 261, 261–62 (2014).

ulate individuals into making choices that benefit companies and not individuals.[244] Emphasizing individual rights to the exclusion of collective governance, too, ignores that many privacy problems—surveillance of neighborhoods or communities, discrimination against particular groups, and chilling minority viewpoints or speech—are collective in nature.[245]

Yet as both sectoral statutory schemes within the United States and contrasting data protection regulation around the world illustrate, operationalizing the HEW Report's principles need not mean idealizing ineffective individual control—especially if individual rights are coupled with more robust systemic regulation.[246]

At the time of the Report, the kind of AI decision-making discussed here was still a hypothetical future.[247] The Report reads as a prescient call for an American version of the right to contest: "Sometimes the individual does not even know that an organization maintains a record about him. Often he may not see it, much less contest its accuracy, control its dissemination, or challenge its use by others."[248]

2. *Due Process Theory and AI Decision-Making.* — One of the only U.S. scholars to directly address the GDPR's right to contestation explicitly rejects it.[249]

---

244. Cohen, What Privacy Is For, supra note 242, at 1925, 1930 ("[Big Data techniques] subject individuals to predictive judgments about their preferences, and the process of modulation also shapes and produces those preferences . . . . [The] emphasis on privatized regulation and control of information flows via notice and choice reinforces precisely those aspects of modulation that are most troubling and most intractable."); see also Woodrow Hartzog, The Case Against Idealising Control, 4 Eur. Data Prot. L. Rev. 423, 426, 429 (2018) [hereinafter Hartzog, The Case Against Idealising Control] (noting that control individuals "are given online is mediated, which means it cannot help but be engineered to produce particular results" and observing that control can be "overwhelming," creating a bandwidth problem); Solove, Privacy Self-Management and the Consent Dilemma, supra note 242, at 1880–82 (noting how privacy self-management relies on consent but does not provide people with meaningful control over their data).

245. See Hartzog, The Case Against Idealising Control, supra note 244, at 430 ("Notions of individual control don't fit well with privacy as a collective value . . . . 'Data privacy is more like air quality or safe drinking water, a public good that cannot be effectively regulated by trusting in the wisdom of millions of individual choices.'" (quoting Zeynep Tufekci, Opinion, The Latest Privacy Debacle, N.Y. Times (Jan. 30, 2018), https://www.nytimes.com/2018/01/30/opinion/strava-privacy.html (on file with the *Columbia Law Review*))); Solove, Privacy Self-Management and the Consent Dilemma, supra note 242, at 1881 ("Privacy costs and benefits . . . are more appropriately assessed cumulatively and holistically—not merely at the individual level.").

246. Kaminski, Binary Governance, supra note 12, at 1579 ("An accountable collaborative governance regime can also complement individual procedural rights. Establishing systemic accountability in a collaborative governance regime can bolster individual rights by providing oversight in the name of affected individuals.").

247. See HEW Report, supra note 68, at 22 ("'Machine intelligence' is a subject with fascinating technical and philosophical aspects. To date, however, there is no evidence that a computer capable of 'taking over' anything it was not specifically programmed to take over is attainable.").

248. Id. at 29.

249. See Huq, A Right to a Human Decision, supra note 8, at 651 ("[N]one of these clusters of reasons provide secure normative ground for a right to a human decision.").

Huq queries whether such a right can be justified. He rejects calls for transparency and accuracy, reasoning that human decision-makers can be just as opaque[250] and just as inaccurate[251] as machines. He rejects dignity as too nebulous a ground for a contestation right.[252] He concludes that none of a host of concerns can justify a right to a human-made decision, even in the criminal law context.[253]

Instead, Huq reasons that the purpose of individualized due process is largely utilitarian: to ensure systemic accuracy and lack of bias.[254] Instead of individual due process challenges, he calls for a "right to a well-calibrated machine decision"—that is, a right to an unbiased and accurate system, rather than a right to engage with its individualized outputs.[255] Such a right could, per Huq, be vindicated through ex ante and systemic measures, or through ex post class action litigation.

We disagree. Challenges aimed at systemic issues are advisable, but cannot replace the ability of individual contestation rights to ameliorate real harms. This section applies the rationales we have identified for individual process in human decision-making—accuracy, rule of law considerations, utilitarianism, natural rights, and, yes, dignity—to decision-making by AI.

Decisions made by AI can be inaccurate. Due process mechanisms can improve the accuracy of the system as a whole.[256] For example, an individual person can best identify when the long-tail problem has occurred.[257] The Somali-American grocers who were not permitted to accept food stamps because the USDA's algorithm mistakenly found fraud could have, through contestation, established that their customers were in fact making

250. See id. at 643 ("Given the availability of mechanisms for investigating machine-learning decisions—some of which parallel methods for understanding human decision making—it cannot be said a priori that machines are any more opaque than humans.").

251. See id. at 654 (arguing that, for the tasks that can be performed by both humans and machines, evidence suggests that machines will generate fewer false positives and negatives than most human decision-making).

252. See id. at 652 ("I also try to avoid tautological reliance on ambiguous and contested concepts such as 'autonomy' and 'dignity.'").

253. Id. at 685. In a second article, Huq does argue for ex post litigation to challenge flawed algorithmic systems, but prefers what he calls "wholesale and not retail" litigation—that is, litigation focused on "system-level operation" of machine-learning tools. Huq, Constitutional Rights in the Machine-Learning State, supra note 8, at 1949. This litigation would complement ex ante regulation and would take the form of agency-directed or class action litigation. Id. at 1950–51.

254. See Huq, Constitutional Rights in the Machine-Learning State, supra note 8, at 1948 ("Indeed, a takeaway from my analysis is that there is a wide array of ex ante tools available to regulators wishing to promote constitutional norms in the machine-learning state.").

255. Huq, A Right to a Human Decision, supra note 8, at 686.

256. Crawford & Schultz, supra note 8, at 121 ("[D]ue process can serve as a systematic management technique for Big Data by uncovering errors, identifying their causes, and providing schemes and incentives to correct them . . . .").

257. For a discussion of the long-tail problem, see supra note 83 and accompanying text.

whole-number purchases.[258] Similarly, individual actions contesting an algorithm's decisions about allocating home care visits for severely disabled individuals revealed both individual and broader inaccuracies.[259] Court proceedings revealed that the algorithm accounted for only about sixty factors from a much longer list collected from patients, didn't account for diabetes issues, and was improperly coded for cerebral palsy.[260] The cerebral palsy mistake alone had "caused incorrect calculations for hundreds of people, mostly lowering their hours [of home care]."[261] Only an individual contestation in which "the other c[ame] and cross-examine[d]"[262] allowed these systemic accuracy problems to be identified.

Individual contestation rights can also support rule of law values. Rule of law values suggest that decisions should be fair, consistent, predictable, and rational across different individuals.[263] But AI decisions can be arbitrary or subject to a logic we cannot understand or normatively reject. For example, an algorithm may find that credit risk correlates to the color of a person's socks.[264] People with pink socks might get better credit than people with blue socks, or vice versa. Even if this correlation is backed by unimpeachable studies, it may still feel unreasonable, arbitrary, or even—if sock color correlates with other features such as gender or sexual orientation—discriminatory.

An individual right to contest AI-made credit decisions could uncover the sock color irrationality. It could uncover, too, whether such rules are being applied consistently across individuals or whether the system instead has created sock color loopholes that make it normatively unfair.

A utilitarian argument for a right to contest AI could take three forms. First, giving individuals a right to contest AI decisions could produce greater acceptance of such decisional systems.[265] Second, where such deci-

258. See generally McGann, supra note 85.

259. See Lecher, supra note 80 (noting how algorithms regarding home visits can work to the detriment of disabled individuals); McCormick, supra note 56 (explaining how disabled and elderly people have had to fight against decisions made by an algorithm to get the support services they need).

260. Lecher, supra note 80.

261. Id.

262. Proverbs 18:17 (NSRV).

263. Crawford & Schultz, supra note 8, at 119.

264. See Ed Felten, What Does It Mean to Ask for an "Explainable" Algorithm?, Freedom to Tinker (May 31, 2017), https://freedom-to-tinker.com/2017/05/31/what-does-it-mean-to-ask-for-an-explainable-algorithm [https://perma.cc/BKJ8-LERE] ("For example, imagine that an algorithm for making credit decisions considers the color of a person's socks, and this is supported by unimpeachable scientific studies showing that sock color correlates with defaulting on credit, even when controlling for other factors."). Felten calls this "unreasonableness." Id.

265. See Tom R. Tyler, Procedural Justice, Legitimacy, and the Effective Rule of Law, 30 Crime & Just. 283, 291 (2003) ("[D]eclining confidence in law and legal authorities may

sions have very significant effects, such as the deprivation of welfare benefits or the denial of child custody,[266] "rule utilitarianism" might suggest that process protections are more likely to maximize social welfare by preventing serious pain. Third, if AI decisions threaten the private sphere, even utilitarians may find that individual process rights should apply. The denial of child custody could be characterized as impinging upon the private sphere;[267] so could, for example, an employer's use of AI to intrusively track employee behavior or attributes.[268]

From a Lockean perspective, individuals should have a right to contest AI decisions where such decisions impinge on natural entitlements such as the rights to life, liberty, and property. A right to contest could help mitigate error. Equally important is that a contestation process could evidence individual buy-in or even consent.

Finally, we come to dignity. The dignitary argument for a right to contest is perhaps the strongest, despite Huq's and others' objections to it. Decisions that affect people's lives implicate dignity. Specific examples are clear on this point. It is offensive to the dignity of Black kidney patients to deny them the same chance at life-saving treatment as white patients with kidney disease of the same severity.[269] It is offensive to the dignity of home-health-care patients to severely limit their existing independence, to leave "people lying in their own waste . . . getting bed sores . . . being shut in . . . skipping meals," and fearing institutionalization, and to "reduce [their] humanity to a number."[270] AI, by its nature, categorizes people in order to make decisions. Categorizing individuals arguably objectifies them; affording a right to contest that categorization restores at least some form of dignity.[271] Affording a right to contest affords a form of respect to

---

lead to declining feelings of obligation to obey the police, the courts, and the law . . . , raising the possibility that compliance may be increasingly problematic."); Tom R. Tyler, What Is Procedural Justice?: Criteria Used by Citizens to Assess the Fairness of Legal Procedures, 22 Law & Soc'y Rev. 103, 128 (1988); see also Selbst & Barocas, Intuitive Appeal, supra note 185, at 1119 ("Tyler and others have shown that people care deeply about procedural justice, to the point that they might find a proceeding more tolerable and fair if their procedural-justice concerns are satisfied even if they do not obtain their preferred outcome in the proceeding.").

266. Dan Hurley, Can an Algorithm Tell When Kids Are in Danger?, N.Y. Times (Jan. 2, 2018), https://www.nytimes.com/2018/01/02/magazine/can-an-algorithm-tell-when-kids-are-in-danger.html (on file with the *Columbia Law Review*).

267. Stephanie Cuccaro-Alamin, Regan Foust, Rhema Vaithianathan & Emily Putnam-Hornstein, Risk Assessment and Decision Making in Child Protective Services: Predictive Risk Modeling in Context, 79 Child & Youth Servs. Rev. 291, 295 (2017).

268. Pegah Moradi & Karen Levy, The Future of Work in the Age of AI: Displacement or Risk-Shifting?, *in* The Oxford Handbook of Ethics of AI 271, 282–83 (Markus D. Dubber, Frank Pasquale & Sunit Das eds., 2020).

269. See Simonite, Kidney Transplants, supra note 64.

270. See McCormick, supra note 56.

271. See Kaminski, Binary Governance, supra note 12, at 1541 ("The dignitary argument—which for U.S. readers skeptical of dignity includes what are often characterized as autonomy concerns—posits that an individual human being should be respected as a whole,

individual people in the system. It permits participation. It establishes agency.

Rather than acting as mere "abstract and vague" concepts, dignity and autonomy interests animate calls for accuracy (to root out harmful mistakes) and rule of law constraints (to root out unequal, inconsistent effects), as well as values of rationality, respect, and individual participation in decision-making. Though dignity and autonomy may not, by themselves, provide sufficient justifications for contestation, they provide essential justifications. And because respecting dignity and autonomy enhances acceptance, including them in design rubrics may ultimately contribute to a decision-making system's legitimacy.

As noted above, dignitary theory is not new to U.S. law. It is not even new in the data privacy context. In fact, early calls for data governance echoed concerns about individual powerlessness and lack of autonomy that sound in similar dignitary notes.[272] These calls resulted in existing U.S. privacy laws that, while not as comprehensive or consolidated as European data privacy law, are founded on the notion that affording transparency and participation mitigates power disparities.

Thus, theories from the due process literature support a call for a right to contest AI. And when we look to the legal systems that have established or suggested establishing a right to contest, we see echoes of each of these theories.

For example, Europe's 1995 Directive protections grew, in part, from a concern about automation bias that sounded in accuracy—that human decision-makers "may attach too much weight" to an automated decision and fail to question its reasoning or catch its errors.[273] The Council of Europe, in its 2020 Recommendation, notes that "algorithmic systems are based on statistical models in which errors form an inevitable part," and that, owing to algorithmic systems' large-scale effects, the "number of people . . . who are affected by these errors and inbuilt bias, will also expand."[274]

Rule of law values, too, animate concerns about algorithmic decision-making. Both the scholarly literature and European policy-makers voice

---

free person. Being subjected to algorithmic decision-making threatens individuals' personhood by objectifying them."); see also supra note 182.

272. See HEW Report, supra note 68, at 223 (noting how there had been little effort to examine new systems' potential to erode privacy and individual autonomy); Daniel J. Solove, A Taxonomy of Privacy, 154 U. Pa. L. Rev. 477, 487 (2006) (referring to the dignitary harms).

273. Mendoza & Bygrave, supra note 10, at 83–84 (quoting Amended Proposal for a Council Directive on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data, at 26, COM (92) 422 final (Oct. 15, 1992)).

274. Council of Eur., Recommendation CM/Rec(2020)1 of the Committee of Ministers to Member States on the Human Rights Impacts of Algorithmic Systems, app. at 4 (2020), https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016809e1154 [https://perma.cc/YC8H-QUTX].

concerns about fairness, predictability, accountability, and the need to discipline algorithmic decisions. The Council of Europe, in its Recommendation, directly invokes the rule of law, admonishing that "the rule of law standards that govern public and private relations, such as legality, transparency, predictability, accountability, and oversight, must also be maintained in the context of algorithmic systems."[275]

Both the GDPR and Council are motivated by autonomy and dignity rationales as well as accuracy.[276] Article 15 of the Directive was, first, intended to protect an autonomy interest that an individual has in actively "participating in the making of decisions which are of importance to [an individual]."[277] The second, closely related, rationale was to protect individual dignity, by preventing machine decisions from being made based on objectified and uncontestable "data shadows."[278]

3. *Open Questions.* — Once we establish that a right to contest should exist, challenging questions remain, such as (1) when are process rights triggered? and (2) what sort of process might each theory require?

The first question—the threshold question—is beyond the scope of this Article and worthy of significant additional work.[279] However, due process theory provides some clues. Each of the theories discussed above suggests that due process is triggered when a significant right of some kind is meaningfully affected. Due process doctrine in practice does the same, asking whether an individual has been deprived of a liberty or property right.[280] The GDPR's right to contestation, similarly, is triggered only when a decision based solely on automated processing, including profiling, produces "legal effects" or "similarly significant effects," or "similarly significantly affects" an individual.[281]

As to the kind of process required, much of the remainder of this Article is dedicated to answering that question. We briefly note here, however, that the arguments for reason giving are particularly salient to our task.[282] AI decisions do not naturally provide reasons for outcomes. In fact,

---

275. Id. at 1.

276. See Mendoza & Bygrave, supra note 10, at 82–83; supra note 182.

277. Mendoza & Bygrave, supra note 10, at 83 (quoting the Commission Proposal for a Council Directive Concerning the Protection of Individuals in Relation to the Processing of Personal Data, at 29, COM (1990) 314 final (Sept. 13, 1990), http://aei.pitt.edu/3768/1/3768.pdf [https://perma.cc/V4Q5-XETS]).

278. Id. at 84 (discerning "a concern to uphold human dignity by ensuring that humans (and not their 'data shadows') maintain the primary role in 'constituting' themselves").

279. See Kaminski, Binary Governance, supra note 12, at 1550–52 (discussing possible thresholds and reserving the question).

280. Mathews v. Eldridge, 424 U.S. 319, 332 (1976); Goldberg v. Kelly, 397 U.S. 254, 263 (1970).

281. GDPR, supra note 13, art. 22(1).

282. See Schauer, Giving Reasons, supra note 207, at 657 ("[W]hen institutional designers have grounds for believing that decisions will systematically be the product of bias . . . or simply excess haste, requiring decisionmakers to give reasons may counteract . . . these tendencies.").

some technologies cannot provide explanations unless they are programmed to do so. Reason giving is central to contestation, not just because it might increase accuracy, but because it commits to treating decisional subjects equally, contributes to consistency, allows for quality control, and demonstrates respect for the subject of a decision.[283] Contestation without an explanation, in other words, is largely meaningless.[284]

Taken all together, the rationales behind individual process rights apply with force to AI decision-making. Effective contestation rights can ameliorate individual harms and give life to broader rule of law values. Contestation can play a valuable role in policing AI decision-making and directing it toward accuracy, consistency, reliability, and fairness.

However, a right to contest by itself is not a panacea. There has been an understandable backlash against mere process, or "procedural fetishism."[285] And as Parts III and IV discuss, effective contestation is heavily dependent on both design and context. Systemic solutions—for example, testing, audits, algorithmic impact assessments, and documentation requirements[286]—are all important, too.[287] Substantive law matters. Access to legal representation or expertise matters. Correcting historic and embedded systemic injustice matters.

The point is not that process alone matters. The point is that it matters, too.

III. CONTESTATION MODELS

Under this normative analysis, the EU, Council of Europe, OECD, Brazil, Quebec, and the Office of the Privacy Commissioner of Canada are all correct in calling for or establishing a right to contest AI. What that right to contest should look like in practice, however, is an open question. The GDPR's right to contest AI, as noted, is more cipher than road map.

The second half of this Article thus turns to how the right to contest might be operationalized. The constitutional due process model, which

283. See id.; see also Hildebrandt, Privacy as Protection of the Incomputable Self, supra note 26, at 109.

284. See Bayamlıoğlu, Transparency of Automated Decisions, supra note 9, at 34.

285. See, e.g., Nicholas Bagley, The Procedure Fetish, 118 Mich. L. Rev. 345 (2019).

286. Desai & Kroll, supra note 176, at 6 (calling for ex ante testing); Selbst, Disparate Impact in Big Data Policing, supra note 59, at 169 (calling for Algorithmic Impact Statements); Selbst & Barocas, Intuitive Appeal, supra note 185, at 1100–05 (calling for algorithmic impact assessments and recoding requirements).

287. Indeed, each of us in different policy contexts has spent a good amount of time and ink discussing a number of them. See Margot E. Kaminski & Gianclaudio Malgieri, Algorithmic Impact Assessments Under the GDPR: Producing Multi-Layered Explanations, 11 Int'l Data Privacy L. 125, 125–26 (2021) [hereinafter Kaminski & Malgieri, Impact Assessments]; Jennifer M. Urban, Joe Karaganis & Brianna L. Schofield, Notice and Takedown in Everyday Practice 133–40 (2017) (U.C. Berkeley Pub. L. Rsch. Paper No. 2755628), https://ssrn.com/abstract=2755628 [https://perma.cc/K2LF-NTBL] [hereinafter Urban et al., Notice and Takedown in Everyday Practice].

affords notice and an opportunity to be heard before a neutral arbiter, encounters significant obstacles when applied to AI decision-making.[288] AI decisions are made at speed and at scale—features that in fact can be core justifications for using AI in the first place.[289] To impose full judicial process on each AI decision would be to impose costs, both monetary and temporal, that might make the use of AI unwieldy.

Sometimes, as in the criminal context, this may be a good thing: The benefits of using AI may be so outweighed by the consequences of potential injustice that nothing short of full judicial process might suffice. Others have, for similar reasons, called for a moratorium on law enforcement use of facial recognition (a form of AI), reasoning that the costs in the law enforcement context are not worth any benefits the technology might afford.[290]

Often, however, AI decision-making may be either so useful or so established that an outright ban is not possible.[291] Affording judicial process in every contestation would outpace the resources of our judicial system.[292] What, then, should be done to afford process that is not perfect, but instead is good enough?

This problem is not new. The question of how to afford adequate individual process at speed and at scale has been at the core of several policy debates.[293] There are "offline" models for abbreviated process, too.[294] This Part identifies and examines four archetypes for process at speed and at scale: the GDPR's right to contestation, the Digital Millennium Copyright Act's "notice-and-takedown" process, the EU's so-called "Right to be Forgotten," and the Fair Credit Billing Act's process for challenging credit

---

288. Scholars who are proponents of individual "due process" in this context have considered ways in which process might be adapted from the traditional model. See, e.g., Citron & Pasquale, Scored Society, supra note 8, at 8; Citron, Technological Due Process, supra note 3, at 1258; Crawford & Schultz, supra note 8, at 107–09 (advocating a procedural data due process model that goes beyond existing government frameworks that rely on ex ante notice, choice, and control).

289. Large-scale online copyright infringement, for example, has prompted both copyright holders and OSPs to use automated tools. See, e.g., Urban et al., Notice and Takedown in Everyday Practice, supra note 287, at 8.

290. See, e.g., Woodrow Hartzog & Evan Selinger, Facial Recognition Is the Perfect Tool for Oppression, Medium (Aug. 2, 2018), https://medium.com/s/story/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66 (on file with the *Columbia Law Review*).

291. For examples of automated decision-making that span sectors as diverse as employment, medical care, and copyright, see the archetypes described infra sections III.B–.E; supra text accompanying notes 50–67.

292. Similarly, Van Loo observes that "[i]t would be unrealistic to require a full trial for every account suspension, even if the risk of error would decrease. We must therefore examine what the burden would be of imposing a given procedure." Van Loo, supra note 5, at 864.

293. Hannah Bloch-Wehba, Global Platform Governance: Private Power in the Shadow of the State, 72 SMU L. Rev. 27, 60 (2019) ("Scholars and civil society organizations have . . . criticized the procedural deficits of global speech governance.").

294. See generally Van Loo, supra note 5, at 851–58 (describing longstanding procedures used by credit card companies and credit bureaus).

card transactions. We show how the GDPR's right to contestation has been implemented by different EU Member States in ways that map onto the archetypes. After establishing these archetypes and observing them in action, this Article turns, in the next and final Part, to crafting a meaningful right to contest AI.

A. *The Design of Privatized Process: Four Contestation Archetypes*

This Part establishes four contestation archetypes, drawn from models used in practice. These archetypes can frame discussions of contestation and provide theoretical clarity to often myopic conversations about process at speed and scale.

In this examination of extrajudicial contestation models, the devil is usually in the details. Contestation varies along a number of axes, with significant consequences for the efficacy and legitimacy of the system. How any one of these axes is calibrated can affect the success of the entire system. For purposes of the archetypes, contestation varies along two key axes; other considerations are addressed in section III.F below.

The first key axis is whether the contestation mechanism itself is established by what we call a "contestation rule" or by a "contestation standard."[295] This distinction is related, but not identical, to the more general distinction between rules and standards in the law. The literature on legal rules and standards is robust.[296] One way to understand the difference between a legal rule and a legal standard is that a legal rule provides clear and precise content ex ante ("do not drive above 75 mph"), while a standard's content is determined by an interpreter ex post ("drive reasonably"—what is reasonable?).[297] Another way to understand the distinction is that a rule ties the hands of future decision-makers, requiring them "to respond in a determinate way to the presence of delimited triggering facts,"[298] while a legal standard provides more discretion, asking decision-makers to apply a "background principle or policy . . . to a fact situation."[299] Rules may have the benefit of being clear and providing notice;[300]

295. See Kaplow, supra note 143, at 559–62. We describe this as a "contestation standard" rather than a "standard" because this could be understood as a rule in a more general sense: It clearly contains some rule-like substance, and it decides there *should* be some sort of contestation right, rather than delegating *whether* there should be such a right to a later decision-maker.

296. E.g., Frederick Schauer, Playing by the Rules: A Philosophical Examination of Rule-Based Decisionmaking in Law and in Life (1991); Colin S. Diver, The Optimal Precision of Administrative Rules, 93 Yale L.J. 65 (1983); Kaplow, supra note 143; Seana Valentine Shiffrin, Inducing Moral Deliberation: On the Occasional Virtues of Fog, 123 Harv. L. Rev. 1214 (2010).

297. Kaplow, supra note 143, at 559.

298. Kathleen M. Sullivan, The Supreme Court, 1991 Term—Foreword: The Justices of Rules and Standards, 106 Harv. L. Rev. 22, 58 (1992).

299. Id.

300. Id. at 62.

standards may have the benefit of avoiding under- or over-inclusivity.[301] Standards also arguably have the benefit of inducing moral deliberation in citizens, including in the corporate context (what is "hostile"? or "offensive"?)[302]—but the corresponding disadvantage of leaving discretion to actors whose interpretations of such broader principles may be self-serving.

A *contestation rule*, as this Article defines it, is similar to a legal rule in that its precise details are spelled out ex ante, by legislators or regulators, including: a notice requirement, a timeline for complaining, a timeline for responses to complaints, or formal requirements for how to complain. A *contestation standard*, by contrast, merely states that there is a right to contest, leaving the procedural details to future decision-makers, private or public.

For example, a law could dictate that "individuals should be afforded a right to contest," without saying more about the parameters of the right, when and how it should be "afforded," and so forth. This would establish what this Article describes as a *contestation standard*, in the sense that without more information, someone other than the legislature will be left to fill in the gaps. At another level, however, a *contestation standard* still provides a legal rule: It establishes that there is a right to contest, rather than leaving that question vague. As another way of distinguishing the concepts, a *contestation rule* may itself contain legal standards—for example, requiring a business to respond to contestation within a "reasonable" time frame. As with legal rules and standards more generally, in practice these are not "pure types," as "legal commands mix the two in varying degrees."[303]

A *contestation rule*, or really, a set of contestation rules, could dictate not just the existence of a right to contest, but its granular details: whether, when, and how notice should be afforded; how decisions should be made; by whom; and on what timeline. For example, a law could state: "Individuals should be notified as to an adverse decision within 5 business days, using the following format, and challenges must be heard before a neutral arbiter within 10 business days, with individuals afforded the following procedural rights."

As with rules and standards more generally, there are costs and benefits to designing a right to contest as more rules based or standards based. A *contestation standard* has the benefit of flexibility. It allows decision-makers to tailor the right in response to particular circumstances, including to particular technologies or sectors. It allows other actors, such as regulators or judges or even regulated entities, to fill in the gaps in the afforded process over time, or to modify approaches as technology, practices, and norms evolve. Thus a contestation standard, like standards more generally, arguably "future-proofs" the law against changing circumstances, requiring less future intervention through legislation or regulation.

---

301. Kaplow, supra note 143, at 590.

302. Shiffrin, supra note 296, at 1227.

303. Kaplow, supra note 143, at 561.

A *contestation rule*, by contrast, has the benefit of clarity. With clarity often comes lower costs. If the law is clear about what it requires, an entity attempting to comply with a contestation rule can spend less money on lawyers and risks fewer penalties for erroneous noncompliance. This has implications for competition: For smaller and less resourced companies, lower-cost rules could establish a more level playing field—although some rules may be costly in their execution and so disadvantage less resourced companies regardless. A contestation rule, too, has the potential benefit of affording less wiggle room. By establishing clear and inflexible processes, a contestation rule can better guarantee that the same process will be afforded equally across all actors.

The second axis along which contestation varies is how much substantive law it incorporates or relies on. A right to contest can be more purely procedural, focused on the mechanics of contestation—on affording a right to contest, but not the underlying substantive rights. Or contestation can be substantive, establishing not just *how* contestation should occur, but *on what basis* a decision may be contested. Simply put, a right to contest that has a substantive focus incorporates not just the procedural rules of a challenge, but the substantive basis of that challenge. For example, a law could state: "Individuals have a right to contest decisions, which cannot be made on the basis of an erroneous piece of data." An individual invoking this right to contest could then challenge a decision for being based on an erroneous piece of data.[304]

The other pole of this axis—contestation based on procedure—might seem strange. How can one have a right to contest a decision that lacks grounding in a substantive right? But when we look to existing models of contestation rights, it becomes apparent that sometimes process is divorced from the substance of the challenge. This can occur in two ways. First, some versions of contestation establish how, procedurally, one might contest a decision, without establishing a substantive basis for the challenge. This is the case for some early implementations of the GDPR's right to contestation. Second, even where there is an underlying substantive basis, other features of a contestation scheme—including strict procedural rules and decision-making at speed and scale—can render the scheme procedural in practice. As described below, this is the case for the notice-and-takedown process of the Digital Millennium Copyright Act (DMCA). In fact, some schemes allow challenges to be made and completed without really getting to any substantive basis for them at all.

For example, a law might state: "Individuals have a right to challenge an AI's decision to assign them a particular grade." This statement establishes only that there is a right to challenge the AI's decision. It does not

304. This is not to say that establishing a substantive basis for contestation makes things simple. The problems with disparate impact cases show that this is no easy task. See, e.g., Ajunwa, Auditing Imperative, supra note 4, at 652–58 (discussing empirical studies of court cases that demonstrate the difficulty of proving disparate impact cases).

establish, normatively or practically, what reasons or reasoning might give rise to successful challenges.

A law that fails to identify the substantive basis for a right to contest leaves substantive decisions in the hands of nonlegislative actors. The substance of a challenge might then be decided not by legislators but by regulators, judges, the contesting parties themselves, or the nonjudicial entities mediating or adjudicating contestation. Or it may afford a right to contest that is all procedure, with no clear substance at all.

Once again, this design choice—whether to make the right to contest more substantive or more procedural—has consequences, both good and bad. The benefit of a right to contest that is more focused on procedure is that substantive law can be subtle, heavily fact dependent, and complicated. Expertise in substantive law can thus be very expensive, which can impede individual access to justice. Additionally, as the due process theory discussed above argues, process can matter for its own sake. Process by itself can afford transparency, reveal problems in decision-making, give individuals agency in a decision, and make decision-making accountable, even if underlying substantive norms go unstated.

There are downsides, though, to a heavily procedural and minimally substantive right to contest. The first is arbitrariness. Affording the ability to contest a decision without substantive grounding gives no notice to the entity whose decisions are subject to contestation, except that it may be subject to challenges against any and all decisions. Unconstrained challenges bring with them costs, including the cost of a large volume of challenges.[305] Arbitrariness can be bad for challengers, too; creating no substantive backstop to a contestation right means that an adjudicator (who is sometimes the same as the entity whose decision is being contested) has untethered discretion.

The following tables illustrate the archetypes. Table I describes the archetypes. Table II offers hypothetical statutory language illustrating them.

TABLE I: THE CONTESTATION ARCHETYPES

	Contestation Standard	Contestation Rule
Procedural Focus	1) Contestation Standard with a Procedural Focus	2) Contestation Rule with a Procedural Focus
Substantive Focus	3) Contestation Standard with a Substantive Focus	4) Contestation Rule with a Substantive Focus

305. See, e.g., Zeran v. Am. Online, Inc., 129 F.3d 327, 333 (4th Cir. 1997) ("[N]otice-based liability for interactive computer service providers would provide third parties with a no-cost means to create the basis for future lawsuits . . . . In light of the vast amount of speech communicated through interactive computer services, these notices could produce an impossible burden for service providers.").

TABLE II: HYPOTHETICAL EXAMPLES OF THE CONTESTATION ARCHETYPES

	Contestation Standard	Contestation Rule
Procedural Focus	1) "An individual shall have a right to contest decisions, and shall be afforded adequate process."	2) "An individual shall have a right to contest decisions. She shall be provided notice of an adverse decision within 5 business days . . . "
Substantive Focus	3) "An individual shall have a right to contest decisions, which shall not be biased."	4) "An individual shall have a right to contest decisions, which cannot be made on the basis of erroneous data points."

As with all archetypes and models, in reality, most laws map onto a continuum, rather than reside at the poles.[306] For example, the GDPR's right to contestation is on its face purely procedural, but read in context, arguably has substantive components.[307] On the spectrum between substantive and procedural, the GDPR's right to contest, at least on its face, sits closer to the procedural pole:

Laws, too, will often contain more than one archetype at a time. For example, the chargeback process of the Fair Credit Billing Act (FCBA) contains both precise language on substance (making it a contestation rule with a substantive focus), and precise rules on the elements of required notice and contestation timelines (making it also a contestation rule with a procedural focus).

Further, laws may operate very differently in practice from how they appear on paper. This can be deliberate—when, for example, a law delegates interpretive power to a regulator that adds in details that make a standard more rule-like in practice. For example, the EU's Right to Be Forgotten has arguably become more rule-like over time, as regulators have issued

306. See, e.g., Jennifer S. Hendricks, In Defense of the Substance-Procedure Dichotomy, 89 Wash. U. L. Rev. 103, 107 (2011) ("Given the linearity of substance and procedure, one could imagine the distinction either as a dichotomy of black and white . . . or as a spectrum of gray, with many or even most legal rules falling in the mushy middle. Descriptively, of course, the latter view is more accurate.").

307. See GDPR, supra note 13, art. 22(3). For example, the right applies to a decision that "significantly affects" the subject of the decision, id. art. 22(1), and the regulators responsible for explaining the articles have clarified that the apparently procedural requirement of a "solely" automated decision in fact involves a determination of whether there was meaningful human involvement, see Guidelines on Automated Individual Decision-Making, supra note 115, at 20–21 (discussing meaningful human involvement).

more detailed guidelines.[308] Similarly, the GDPR's right to contestation has been altered by Member States whose implementations of the right have moved it from one quadrant to another.[309]

Or, the law's implementation might change over time to depart from its original design. For example, some online platforms have developed approaches to online copyright infringement that one of us has termed "DMCA Auto" and "DMCA Plus."[310] In these approaches, online service providers (OSPs) employ automated systems to remove content—or prevent it from ever making it onto the provider's platform. Some versions of these approaches forgo substantive review in favor of rapid removal at scale; others go beyond what is required by the DMCA in the first place.[311] In turn, these decisions are sometimes subject to a privatized version of contestation that also departs from the law.[312] On paper, then, the DMCA establishes a contestation rule with a procedural focus, grounded in substantive copyright law. But what happens in practice may depart from the substantive law; in the case of "DMCA Plus," practice may depart from the DMCA's procedural requirements, too.

This brings us to an important aspect of our chosen archetypes: Each is an example of privatized contestation—contestation effected by private parties. In each chosen archetype, the private parties that actually apply a contestation scheme develop that scheme and operate under some type of

---

308. See Eur. Data Prot. Bd., Guidelines 5/2019 on the Criteria of the Right to Be Forgotten in the Search Engine Cases Under the GDPR (Part 1), paras. 13–83 (July 7, 2020), https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201905_rtbfsearchengines_afterpublicconsultation_en.pdf [https://perma.cc/6SVM-V474] (detailing grounds for a data subject's personal data to be delisted from search engine results and grounds for a search engine's proper refusal to delist such data); see also Article 29 Data Prot. Working Party, Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja Gonzáles" C-131/12, at 2–3 (2014), http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf [https://perma.cc/98GH-6SPR] [hereinafter Article 29 Working Party, Guidelines on Google Spain] (listing circumstances under which data subjects can demand that "search engines . . . de-list certain links to information affecting their privacy from the results for searches made against their name").

309. See Malgieri, Automated Decision-Making in the EU Member States, supra note 115, at 18–23 (comparing member state implementations).

310. Urban et al., Notice and Takedown in Everyday Practice, supra note 287, at 29; see also Maria Strong, U.S. Copyright Off., Section 512 of Title 17: A Report of the Register of Copyrights 67 (2020), https://www.copyright.gov/policy/section512/section-512-full-report.pdf [https://perma.cc/7C68-HWFA] (noting the existence of "DMCA+ systems"); Annemarie Bridy, Copyright's Digital Deputies: DMCA-Plus Enforcement by Internet Intermediaries, *in* Research Handbook on Electronic Commerce Law 185, 187 (John A. Rothchild ed., 2016) (surveying "the current landscape of DMCA-plus enforcement").

311. Urban et al., Notice and Takedown in Everyday Practice, supra note 287, at 29.

312. See Bridy, supra note 310, at 197 (explaining how YouTube's Content ID program and Vimeo's Copyright Match program "allow users to dispute a copyright owner's claim on content").

statutory or regulatory framework. Some readers might characterize these choices as leaving a missing box: privatized contestation unconstrained by law or regulation. For example, much ink has been spilled on the Communications Decency Act (CDA) Section 230 and the broad immunity it affords to platforms from liability for online content moderation.[313] In the absence of a statutory contestation mechanism for most online content, many platforms have developed contestation schemes that are constrained only by the platforms' preferences and interests.[314] Those purely privatized mechanisms can certainly inform the conversation about how to design contestation rights—especially whether or not companies can be trusted to come up with adequate process and substance. However, this Article aims to structure a conversation about statutory and regulatory design rather than entirely privatized approaches.[315]

The rest of this Part turns to examples that illustrate these archetypes of contestation in action. Table III identifies how our examples map onto our contestation archetypes.

TABLE III: THE CONTESTATION ARCHETYPES IN ACTION

	Contestation Standard	Contestation Rule
Procedural Focus	1) The GDPR's "Right to Contestation"	2) The Digital Millennium Copyright Act's (DMCA's) "Notice-and-takedown" regime; The UK Right to Contestation
Substantive Focus	3) The EU's "Right to Be Forgotten" (RTBF); The Slovenian Right to Contestation	4) The Fair Credit Billing Act (FCBA); The French & Hungarian Rights to Contestation

313. E.g., Danielle Keats Citron, Hate Crimes in Cyberspace 170–81 (2016); Eric Goldman, An Overview of the United States' Section 230 Internet Immunity, *in* The Oxford Handbook of Online Intermediary Liability 155, 155 (Giancarlo Frosio ed., 2020); Jeff Kosseff, The Twenty-Six Words That Created the Internet (2019); David S. Ardia, Free Speech Savior or Shield for Scoundrels: An Empirical Study of Intermediary Immunity Under Section 230 of the Communications Decency Act, 43 Loy. L.A. L. Rev. 373 (2010); Danielle Keats Citron & Benjamin Wittes, The Internet Will Not Break: Denying Bad Samaritans § 230 Immunity, 86 Fordham L. Rev. 401 (2017); Eric Goldman, The Ten Most Important Section 230 Rulings, 20 Tul. J. Tech. & Intell. Prop. 1 (2017); Felix T. Wu, Collateral Censorship and the Limits of Intermediary Immunity, 87 Notre Dame L. Rev. 293 (2011).

314. See Kate Klonick, The Facebook Oversight Board: Creating an Independent Institution to Adjudicate Online Free Expression, 129 Yale L.J. 2418, 2427–48 (2020) (discussing Facebook's content moderation process prior to the establishment of the firm's Independent Governance and Oversight Board); Van Loo, supra note 5, at 832 (providing "case studies of the dispute processes designed by Airbnb, Amazon, Facebook, and Google").

315. Inasmuch as reforms to CDA 230 suggest implementing statutory changes, these archetypes may prove useful.

In the wild, none of these examples is perfect. Here, each is simplified for purposes of illustration. At their core, however, these examples effectively illustrate the variations in how a right to contest might be designed.[316]

B. *Archetype 1 Illustrated: The GDPR's Right to Contestation*

The first quadrant of the contestation archetypes is a *contestation standard* with a *procedural focus*.[317] The GDPR's right to contestation embodies this archetype.

As discussed above, the GDPR's right to contestation is a set of standards rather than specific rules. It does not, on its face, provide substantive grounds for challenging algorithmic decisions—those grounds, some suggest, will be found in other areas of substantive law.[318] The Guidelines issued by the EU's data regulator, the European Data Protection Board, highlight the centrality of the right to contest without giving it much further substance.[319]

While the right to contestation itself is as of yet a cipher, other GDPR rights can be understood to give it substance. For example, a number of the GDPR transparency rights are meant to enable contestation.[320] The GDPR requires notice to individuals who have been subjected to an automated decision; disclosure of "meaningful information about the logic involved" in an automated decision-making system; and explanation of individual decisions.[321] These various forms of transparency are intended to enable individuals to meaningfully contest algorithmic decision-making.[322]

---

316. The newly enacted Virginia Consumer Data Privacy Act, Va. Code § 59.1-577(C) (2021), and Colorado Privacy Act, 2021 Colo. Sess. Laws 3445, 3459 (to be codified at Colo. Rev. Stat. § 6-1-1306(3) (2021)), each contain privatized contestation models for "personal data rights" that could be slotted into the archetypes.

317. To be clear, this is what the GDPR right to contest looks like on the face of the law. Certain EU Member States have further detailed this right, sometimes in ways that move it from this first archetype to one of the other quadrants. For further discussion of this hybridization, see infra section III.F.

318. Bayamlıoğlu, Transparency of Automated Decisions, supra note 9, at 41–49 (observing that "[n]either Article 22 nor the GDPR in general[] contains any guidance as to the substance of the right to contest automated decisions" and arguing that the contents of the right of contestation can be "a legal procedure or an adjudicatory system").

319. Id. at 41.

320. The right to explanation and the right to know "meaningful information about the logic involved," GDPR, supra note 13, art. 15(1)(h), in automated decision-making are, according to the Guidelines, meant to empower individuals to contest such decisions, Guidelines on Automated Individual Decision-Making, supra note 115, at 27; see also Mendoza & Bygrave, supra note 10, at 91; Selbst & Powles, supra note 127, at 236 ("[T]he test for whether information is meaningful should be functional, pegged to some action the explanation enables in the data subject, such as the right to contest a decision as provided by Article 22(3).").

321. Kaminski, Right to Explanation, Explained, supra note 25, at 196–200.

322. Id. at 211.

Generally applicable GDPR rights also give meaning to, or complement, the right to contestation.[323] For example, the right to access, which includes a right to see both the data a company holds about an individual and inferences a company has made, enables individuals to challenge a decision as being based on incorrect data or incorrect inferences.[324] The GDPR contains a correction right (the "right to rectification") as well, which enables individuals to require companies to correct inaccurate personal data.[325] Several other generally applicable GDPR rights, such as the right to erasure, right to object, and right to restrict processing,[326] can each be understood as alternatively (1) complements to the right to contestation, (2) minimum requirements regardless of the strength of the contestation right, or perhaps (3) as models for the contestation right.

The right to contestation is intertwined, too, with the GDPR's treatment of the "human in the loop" of automated decision-making.[327] For reasons ranging from a concern about respecting human dignity[328] to a concern about excessive deference to automated decisions,[329] the GDPR pushes both private and public entities toward involving humans in significant decisions, rather than allowing such decisions to be made by machines alone. If companies wish to escape Article 22's safeguard requirements, they have to meaningfully involve a human in the loop.[330]

Where Article 22 applies, companies must adopt a means for "human intervention."[331] The Guidelines suggest this might mean "for example providing a link to an appeals process at the point the automated decision is delivered to the data subject, with *agreed timescales* for the review and a *named contact point* for any queries."[332] This suggestion in some ways resem-

323. See Edwards & Veale, supra note 175, at 49.

324. GDPR, supra note 13, art. 15(1); see also Guidelines on Automated Individual Decision-Making, supra note 115, at 17.

325. GDPR, supra note 13, art. 16; see also Edwards & Veale, supra note 175, at 38.

326. GDPR, supra note 13, arts. 17, 18, 21.

327. Jones, The Right to a Human in the Loop, supra note 72, at 231.

328. Id.; see also Mendoza & Bygrave, supra note 10, at 84 (noting "a concern to uphold human dignity by ensuring that humans (and not their 'data shadows') maintain the primary role in 'constituting' themselves"); Zarsky, Incompatible, supra note 182, at 1016–17 ("[W]hen faced with crucial decisions, a human should be treated with the dignity of having a human decision-maker address his or her personal matter.").

329. Mendoza & Bygrave, supra note 10, at 84; Bygrave, Minding the Machine, supra note 10, at 18; Citron, Technological Due Process, supra note 3, at 1271–72.

330. First, Article 22's scope and stringency incentivize companies to meaningfully involve humans in algorithmic decision-making. Recall that Article 22 applies only when decisions are "based solely on automated processing"; this has been interpreted in the Guidelines to mean decisions that do not involve meaningful human involvement and oversight. Guidelines on Automated Individual Decision-Making, supra note 115, at 20–21 (discussing what constitutes "meaningful human involvement").

331. GDPR, supra note 13, art. 22(3).

332. Guidelines on Automated Individual Decision-Making, supra note 115, at 32.

bles the DMCA notice-and-takedown process, in that it establishes a company contact point and suggests that there be timescales for procedures, although it does not establish specific timelines.

Also notable is that the Guidelines' example does not involve an external neutral decision-maker but houses the appeals process within the same company that implements automated decision-making.[333] While this guidance arguably moves the right to contest from a pure contestation standard to something more rule like, it still leaves most details up to the entity processing the AI decision. Moreover, it is an example, not a requirement.

The central concern about the right to contestation is that, like its predecessor, it may become dead-letter law.[334] The Guidelines, however, show[335] that the regulators that enforce the GDPR believe contestation is a core component of the GDPR's basket of rights.

A second concern about the right to contestation as a contestation standard is that it leaves substantial wiggle room for companies and governments to render the right ineffective in practice. Furthermore, the GDPR allows Member States to implement their own versions of the right.[336] As a standard, Article 22 leaves ample room for Member States to craft their own versions of the contestation right, potentially resulting in both higher compliance costs for companies operating across the EU and in varying degrees of efficacy that depend on where a person lives.

Finally, the GDPR right at first appears to be largely procedural rather than substantive. It is not clear from the text *on what basis* someone may contest an AI decision. This leaves open the possibility that implementing entities or Member States can construct a right that is almost entirely procedural. And in fact, both the Guideline example discussed above and the implementation by some Member States discussed below have construed the right to contestation as being largely procedural in nature. This risks defanging the right and allowing companies to comply through rubber-stamped processes rather than requiring effective mechanisms with meaningful effects.[337]

But there are strong arguments that when it is read in context, there is a substantive backstop to the GDPR's contestation right—illustrating

333. Cf. Citron & Pasquale, Scored Society, supra note 8, at 20 (proposing that the FTC plays an analogous supervisory role in the context of credit-scoring algorithms); Crawford & Schultz, supra note 8, at 126–27 (proposing that a regulatory entity like the FTC play this role).

334. Edwards & Veale, supra note 175, at 65–67; Wachter et al., Why a Right to Explanation of Automated Decision-Making Does Not Exist, supra note 115, at 96–97.

335. Malgieri, Automated Decision-Making in the EU Member States, supra note 115, at 4.

336. GDPR, supra note 13, art. 22(2)(b).

337. Wachter & Mittelstadt, Right to Reasonable Inferences, supra note 120, at 569 (calling "into question that the right to contest can be meaningfully implemented without underlying decision-making standards").

that laws often fall on a spectrum between the poles rather than existing as pure versions of the archetypes. At least, individuals can contest the inaccuracy of the personal data on which decisions are based, using the general GDPR right to rectification.[338] It is clear, too, that the right to contest is intended to go beyond mere rectification. Like other restrictions on AI decision-making, the right is intended to protect "the data subject's rights and freedoms and legitimate interests."[339] One can thus argue that the GDPR affords a right to contest not just erroneous decisions, but biased and discriminatory decisions, and most decisions based on highly sensitive personal data.[340] There is the worrisome prospect that both complying entities and Member States will eschew this substantive grounding and take the GDPR's right to contest in the more proceduralized direction offered in the Guidelines.

C. *Archetype 2 Illustrated: The DMCA's "Notice-and-Takedown" Process and the UK Right to Contestation*

We now move to the second archetype: a *contestation rule* with a *procedural focus*. This is illustrated by some implementations of the influential "notice-and-takedown" process created by section 512 of the U.S. DMCA.[341] We also offer the UK implementation of the GDPR's right to contestation as an example.

1. *DMCA Section 512.* — The DMCA's section 512 contains one of the most widely adopted versions of a contestation right in the digital age. The DMCA's approach has been exported in various forms throughout the world,[342] including in the implementation of the EU's E-Commerce

338. GDPR, supra note 13, art. 16 ("The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her.").

339. Id. art. 22(3).

340. GDPR, supra note 13, Recital 71. Recital 71 explains that entities should aim to minimize errors and to "prevent . . . 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," and to not utilize processing "that results in measures having such an effect." While not specifically directed at the contestation right, these substantive goals can be understood as the goals of contestation as well. Additionally, Recital 71 states that AI decisions based on particularly sensitive personal information ("special categor[y]" data, such as biometric data, racial data, and sexual orientation data) "should be allowed only under specific conditions."

341. 17 U.S.C. § 512 (2018).

342. For a detailed account of the DMCA's influence on other implementations, see Urban et al., Notice and Takedown in Everyday Practice, supra note 287, at 21–23 ("The E-Commerce Directive was largely inspired by the DMCA safe harbors, though it differs from the DMCA in several notable ways."). For comprehensive discussions of the background and relationship between the U.S. and European approaches, see generally Aleksandra Kuczerawy, Intermediary Liability and Freedom of Expression in the EU: From Concepts to Safeguards (2018); Miquel Peguera, The DMCA Safe Harbors and Their European Counterparts: A Comparative Analysis of Some Common Problems, 32 Colum. J.L. & Arts

Directive.[343] For better or worse, section 512 has become a worldwide model for a privatized version of individual due process as applied to online expression.[344]

Section 512 structures online copyright disputes. Its drafters sought to reduce legal uncertainty for OSPs and to reduce costs for copyright holders facing online copyright infringement.[345] Under section 512, copyright holders can address online copyright infringement by sending relatively inexpensive "takedown" notices directly to OSPs.[346] If OSPs respond to the takedown notices by removing the allegedly infringing material, they receive "safe harbor" from certain types of secondary liability for their users' copyright infringements.[347] In turn, targets of takedown notices can contest removal by sending a "counter notification" asking that material be reinstated.[348]

Section 512's notice-and-takedown scheme, taken as a whole, exemplifies a contestation rule. If material infringes copyright, then it comes down. Moreover, the statute dictates many (though notoriously not all) precise elements of a tightly orchestrated process.[349] Copyright holders

---

481, 511 (2009) (arguing that, while the EU and U.S. statutes include problematic ambiguities and other similarities, their differences render them functionally distinct).

343. Council Directive 2000/31, art. 14, 2000 O.J. (L 178) 1, 13 (EC) [hereinafter E-Commerce Directive]. Note that, in the majority of implementations, "takedown" is reserved for copyright complaints, though it is sometimes applied to other serious complaints (such as complaints of so-called "manifestly unlawful" speech), and rarely, to any unlawful content. See Aleksandra Kuczerawy, From 'Notice and Take Down' to 'Notice and Stay Down': Risks and Safeguards for Freedom of Expression, *in* The Oxford Handbook of Intermediary Liability Online 525, 526 (Giancarlo Frosio ed., 2020) (comparing and contrasting some specific national implementation strategies and how they "can impact the right to freedom of expression").

344. Beyond the E-Commerce Directive, the DMCA has influenced approaches in online service providers' mechanisms for removing content that implicates issues other than copyright. See, e.g., Report a Trademark Issue, Twitter, https://support.twitter.com/forms/trademark [https://perma.cc/A8HF-W8BF] (last visited Aug. 2, 2021); Trademark Report Form, Facebook, https://www.facebook.com/help/contact/284186058405647 [https://perma.cc/42ES-JWFA] (last visited Aug. 2, 2021).

345. H.R. Rep. No. 105-551, pt. 2, at 49–50 (1998); S. Rep. No. 105-190, at 20 (1998). For a comprehensive account of the reasoning behind, and debates surrounding, the passage of the DMCA, see generally Jessica Litman, Digital Copyright: Protecting Intellectual Property on the Internet (2001).

346. 17 U.S.C. § 512(c)(3); S. Rep. No. 105-190, at 45 (explaining how the "notice and takedown" procedure of subsection (c)(3) is a "formalization and refinement" of the cooperative process meant to efficiently handle network-based copyright infringement).

347. 17 U.S.C. § 512(c)(1)(C); S. Rep. No. 105-190, at 19 (explaining that under section 512, there are a series of "safe harbors" for certain common activities of OSPs, in which the OSP receives the benefit of limited liability).

348. 17 U.S.C. § 512(g)(2)(B).

349. A number of aspects of section 512 have been the subject of expensive and time-consuming litigation, once again illustrating that most real-life examples sit on a spectrum rather than being a pole of the archetypes. Even the timeline for takedown itself contains, in addition to precise rules, standards such as "act[] expeditiously to remove" material. Id. § 512(c)(1)(A)(iii).

must send a takedown request that contains specific information.[350] If a copyright holder properly requests a takedown, OSPs must "respond[] expeditiously to remove" material.[351] Those whose material is targeted by a takedown notice can contest removal by sending a "counter notification"—that, again, contains specified information[352]—back to the OSP.[353] If a counternotice arrives, the OSP must forward it on to the notice sender, who can choose to file a copyright lawsuit against the target or let the dispute go.[354] If, after a statutorily prescribed time period (ten to fourteen days), no lawsuit is filed, the OSP must replace the targeted material.[355]

Viewed as it is applied in practice, section 512 also exemplifies a procedural focus. Section 512's contestation mechanism, in theory, is grounded in substantive copyright law. Takedown and "putback" should turn on copyright infringement or noninfringement, respectively. And in some circumstances, this is how it operates: OSPs review takedown requests and consider whether there is infringement, then decide whether to remove the complained-of material.[356]

In other cases, however, the notice-and-takedown project is, in practice, almost entirely procedural. In these circumstances, notices arrive and material is removed with little or no substantive review by OSPs.[357] This occurs for a number of reasons. First, some OSPs must manage notices at scale—millions, or at the limit, even a billion or more notices in a year. For these OSPs, automated review and takedown is the only practicable option.[358]

Second, the notice-and-takedown system creates an interlocking set of requirements, incentives, and risks that push OSPs away from substantive review and toward takedown. To begin, a copyright holder sending a takedown notice does not have to prove a copyright violation. They just have to identify allegedly infringing materials and state that they believe in good faith that the targeted use is not authorized.[359] OSPs reviewing the notice then have strong incentives to err on the side of removal, because strong remedies—injunctions, stiff statutory damages, and attorneys'

350. Id. § 512(c)(3) (specifying the required "[e]lements of notification").

351. Id. § 512(c)(1)(C). This, of course, is a standard embedded within a largely rule-bound process. As noted, none of the archetypes is a perfect example.

352. Id. § 512(g)(3) (specifying the "[c]ontents of counter notification").

353. Id. § 512(g)(2)(B).

354. Id. § 512(g)(2)(B)–(C).

355. Id.

356. See Urban et al., Notice and Takedown in Everyday Practice, supra note 287, at 40–41 (noting that these relatively substantively-based processes are still designed and followed by the OSPs, which are not neutral arbiters).

357. Id. at 54–55.

358. See id. at 52–54 (explaining that "notice-and-takedown" policies range from using human review to evaluate manageable numbers of requests to processing mass amounts of notices using automated systems).

359. 17 U.S.C. § 512(c)(3)(A).

fees—are available for copyright infringement.[360] Some OSPs thus simply comply with all notices that appear to conform with section 512's procedural requirements.[361] As an OSP representative put it in empirical work by one of us, "[T]he process forces you to try to stay out of making judgment calls [and] to take [takedown requests] at face value."[362]

In these situations, the online platform either engages in a substantive analysis biased by the incentives in the system or does not engage in substantive copyright analysis at all. Instead, the law establishes a statutorily dictated process that is implemented by nonneutral parties, acting against a legal and practical backdrop that militates toward takedown.

Section 512(f), which provides a judicial backstop to the process, allows participants to sue one another for knowing material misrepresentations that result in content being improperly removed or restored.[363] That is, section 512(f) does tether the notice-and-takedown process to the substance of copyright law—and provides recourse to a neutral arbiter—but only inasmuch as it prevents users of the process from knowingly misrepresenting the law, and only inasmuch as it is actually invoked in practice (which isn't much). In the end, the ability to recover damages under section 512(f) pales in comparison to the downside risk OSPs incur by refusing removal or replacing contested material.[364]

On its face, the section 512 process is carefully structured to balance responsibilities and protect the rights of both copyright holders and notice targets. By some measures, section 512 has been extraordinarily successful. Its takedown process has been followed an estimated billions of times over the last twenty years,[365] relatively inexpensively resolving disputes and clearing infringing material from the internet. Measured by the myriad of online dispute resolution processes that mimic its structure,[366] it is also wildly successful as a model.

---

360. Statutory damages range from $200 to $150,000, per work infringed. Id. § 504(c)(2). Because statutory damages are calculated per work infringed, OSPs, which may host or link to very large numbers of user-posted works, can face extremely high potential awards. For a detailed discussion of the effect of statutory damages in the U.S. copyright system, see Pamela Samuelson & Tara Wheatland, Statutory Damages in Copyright Law: A Remedy in Need of Reform, 51 Wm. & Mary L. Rev. 439, 452 (2009) (observing that the "new higher range for statutory damages that could be awarded against willful infringers . . . unfortunately opened up opportunities for excessive awards far beyond congressional intent").

361. Urban et al., Notice and Takedown in Everyday Practice, supra note 287, at 41.

362. Id.

363. 17 U.S.C. § 512(f).

364. Statutory damage awards are potentially so high that some OSP decisions not to remove disputed material may fairly be characterized as "betting the company." Urban et al., Notice and Takedown in Everyday Practice, supra note 287, at 43. OSPs also consider the slowness and expense of court cases, and the high burden of proof required by section 512(f), to be stymieing. Id.

365. Id. at 8.

366. See supra notes 342–344 and accompanying text.

Yet section 512 attracted due process concerns from its inception.[367] Copyright holders have complained that the takedown process is insufficiently effective, too costly, and burdensome.[368] OSPs have argued that section 512's process risks capturing legal uses along with infringing materials.[369] The "counternotice" mechanism was added late in the legislative process in response to process concerns.[370] Some have pointed out that the required ten-to-fourteen-day takedown period could quell time-sensitive speech; others have observed that it gave the notice sender little time to file a lawsuit if a counternotice arrived.[371] Civil society groups have worried that section 512's contestation mechanisms and other design features are insufficient to deter abusive or mistaken removals.[372]

The DMCA's due process protections thus appear to be shaky. Although the lack of public visibility into the system makes it impossible to fully observe, there is now a small body of empirical research into the notice-and-takedown process[373] and stakeholder experiences.[374] The U.S. Copyright Office, too, recently completed a multiyear study of the section 512 system.[375] Investigators consistently have found mistaken or improper uses of the takedown system. In 2006, one of us found that 29% of a sample of notices to Google Search were flawed.[376] In 2017, one of us found that 31% of a large sample of notices sent to Google Search were questionable. In that same sample, 70% of the notices sent to Google Image Search were fundamentally flawed, largely because of one prolific sender.[377] Without

367. See Jennifer M. Urban & Laura Quilter, Efficient Process or "Chilling Effects"? Takedown Notices Under Section 512 of the Digital Millennium Copyright Act, 22 Santa Clara Comput. & High Tech. L.J. 621, 633–36 (2006).

368. Strong, supra note 310, at 77–82.

369. Id. at 139–41; Urban et al., Notice and Takedown in Everyday Practice, supra note 287, at 39–43.

370. See Urban & Quilter, supra note 367, at 633–36.

371. Id. at 636–37.

372. Id.; Strong, supra note 310, at 11.

373. E.g., Sharon Bar-Ziv & Niva Elkin-Koren, Behind the Scenes of Online Copyright Enforcement: Empirical Evidence on Notice & Takedown, 50 Conn. L. Rev. 339 (2018); Perel & Elkin-Koren, supra note 159, at 473; Daniel Seng, The State of the Discordant Union: An Empirical Analysis of DMCA Takedown Notices, 18 Va. J.L. & Tech. 369 (2014); Urban & Quilter, supra note 367; Urban et al., Notice and Takedown in Everyday Practice, supra note 287; Jennifer M. Urban, Brianna L. Schofield & Joe Karaganis, Takedown in Two Worlds: An Empirical Analysis, 64 J. Copyright Soc'y U.S.A. 483 (2017) [hereinafter Urban et al., Takedown in Two Worlds]; Rishabh Dara, Intermediary Liability in India: Chilling Effects on Free Expression on the Internet, Ctr. For Internet & Soc'y (2011), http://cis-india.org/internet-governance/intermediary-liability-in-india.pdf [https://perma.cc/TL9G-LWDC].

374. E.g., Jennifer M. Urban, Joe Karaganis & Brianna L. Schofield, Notice and Takedown: Online Service Provider and Rightsholder Accounts of Everyday Practice, 64 J. Copyright Soc'y U.S.A. 371 (2017) [hereinafter Urban et al., Accounts of Everyday Practice]; Urban et al., Notice and Takedown in Everyday Practice, supra note 287.

375. Strong, supra note 310.

376. Urban & Quilter, supra note 367, at 667.

377. Urban et al., Takedown in Two Worlds, supra note 373, at 499, 510.

her notices, 36% were questionable. Also in 2017, Sharon Bar-Ziv and Niva Elkin-Koren investigated the Israeli (.il) notices from the same sample, discovering that only 34% contained allegations of copyright infringement; the other 66% were improper subject matter.[378]

The DMCA's contestation mechanisms thus apparently have failed to fulfill their purpose. Despite evidence that improper or questionable removals are not uncommon, counternotices appear to be rare; section 512(f) suits for any party's knowing material misrepresentation of a copyright violation are even rarer.[379] The counternotice mechanism is used extremely infrequently;[380] OSPs largely consider it a dead letter.[381] The Copyright Office's study, too, uncovered problems with the counternotice process.[382] The DMCA thus has lessons to teach about what to avoid, or to include, when designing contestation.

2. *The UK Implementation of the Right to Contestation.* — The UK implementation of the GDPR's right to contestation offers a second example of a contestation rule with a procedural focus. In implementing the GDPR before Brexit, the UK adopted a highly proceduralized approach to challenging algorithmic decision-making. This approach builds on domestic law in place before the GDPR.383

Prior to the GDPR, section 12 of the UK Data Protection Act of 1998 required a company to notify individuals of an automated decision "as soon as reasonably practicable" and provided individuals twenty-one days to request reconsideration or request a new decision with human involvement.[384] A company then had to respond within twenty-one days with "a

---

378. Bar-Ziv & Elkin-Koren, supra note 373, at 359–60.

379. Because no public record of counternotices exists, it is impossible to know exactly how often they are sent; however, all available evidence indicates they are rare. Most quantitative work focuses on notices to search engines, which are less likely to receive counternotices because they are not required to forward notices to the targets. See, e.g., Seng, supra note 373; Urban & Quilter, supra note 367, at 626; Urban et al., Takedown in Two Worlds, supra note 373, at 393. Relying on studies of search alone would likely result in an underestimate of counternotices. However, a qualitative study of OSPs and large notice senders, covering a wide range of OSP types, also found counternotices to be rare. Urban et al., Notice and Takedown in Everyday Practice, supra note 287, at 44–46.

380. Urban et al., Accounts of Everyday Practice, supra note 374, at 394.

381. Id.

382. Strong, supra note 310, at 162 ("Another aspect of section 512 that received significant attention . . . was the ten–fourteen day period between when the OSP receives a counter-notice and when the copyright holder must file a federal lawsuit or see the material get replaced set forth in section 512(g)(2)(C).").

383. See Malgieri, Automated Decision-Making in the EU Member States, supra note 115, at 9–10 (noting that the UK's 2018 Data Protection Act's proceduralized process for contesting algorithmic decision-making is probably due to previous provisions of the UK Data Protection Act of 1998).

384. UK Data Protection Act 1998, c. 29, § 12(2)(b) (UK) ("[T]he individual is entitled, within twenty-one days of receiving that notification from the data controller, by notice in writing to require the data controller to reconsider the decision or to take a new decision otherwise than on that basis.").

written notice specifying the steps that [it] intends to take to comply with the [individual's] notice."[385] Nothing in the law specified what measures a company needed to take to adequately reconsider a decision. Thus, the UK approach to algorithmic decision-making, prior to the GDPR, was to focus on procedural timelines and not on substantive prohibitions or on standards for reversing decisions.

New UK law implementing the GDPR extended the twenty-one days to one month. As before, a company must notify an individual of an automated decision in writing "as soon as reasonably practicable"; the individual has one month (instead of twenty-one days) to request that a company "(i) reconsider the decision, or (ii) take a new decision that is not based solely on automated processing."[386] The company then ordinarily has a month to "consider the request, including any information provided by the data subject . . . comply with the request, and . . . by notice in writing inform the data subject of: (i) the steps taken to comply with the request, and (ii) the outcome of complying with the request."[387] This process may be amended through regulation.[388] This establishes what Gianclaudio Malgieri has referred to as a "proceduralized explanation"—individuals are given insight into the process of contestation, which may itself check company behavior, or even incentivize pro-consumer outcomes through transparency.

Other implementing EU Member States also specify some procedural requirements for contestation, though not to the same level of detail as the UK. Ireland and France invoke appellate procedure.[389] Ireland requires companies to enable an individual to "(I) make representations to the controller in relation to the decision, (II) request human intervention in the decision-making process, [and] (III) request to appeal the decision."[390] As in the UK, companies must "notify the [individual] in writing

385. Id. § 12(3).

386. UK Data Protection Act 2018, c. 12, § 14(4)(a)–(b) (UK).

387. Malgieri, Automated Decision-Making in the EU Member States, supra note 115, at 9 n.80 (quoting UK Data Protection Act 2018, § 14(5)) ("Section 14(5) states that the data controller must react within the period described in Article 12(3), GDPR[,] . . . which commences] within one month of receipt of the request . . . [and] may be extended by two further months where necessary.").

388. According to Malgieri, these safeguards in the UK law "basically absorb[]" the GDPR safeguards of contestation, expressing their point of view, and getting human intervention. Id. at 10. Under this interpretation, the UK has implemented the right to contestation as a right to "reconsider the decision"; the right to obtain human intervention as the right to "[t]ake a new decision that is not based solely on automated processing"; and the right to express one's voice as the right to have a company consider "any information provided by the [individual]." Id. at 10.

389. See id. at 10–11, 13, 15.

390. Data Protection Act 2018, § 57(1)(b)(ii) (SI 7/2018) (Ir.).

of (i) the steps taken to comply with the request, and (ii) in the case of an appeal . . . the outcome of the appeal."[391]

It is too early to know how these proceduralized implementations of Article 22 will fare, but the DMCA suggests some lessons. Section 512's detailed timelines and requirements for notices and counternotices have not, for the most part, created a usable contestation process. Instead, both the process as actually practiced and substantive decisions turn on OSPs, which are influenced by their analysis of liability risk. Without substantive standards for reconsideration or guidance on how to treat additional information provided by the data subject, it is unclear whether procedures alone will enhance accuracy and prevent discrimination or respect dignity. Similarly, the UK law's transparency requirements require a description of the procedural steps themselves, not the underlying reasons for a decision.[392] This is process giving, not reason giving. By itself, the UK rubric is unlikely to foster the consistency and reliability, or serve the decision-disciplining functions, that we expect from adequate process.

D. *Archetype 3 Illustrated: The "Right to Be Forgotten" and the Hungarian and Slovenian Rights to Contestation*

To illustrate our third archetype, a *contestation standard* with a *substantive focus*, we turn to the EU's so-called "Right to Be Forgotten." We additionally point to the Hungarian and Slovenian implementations of the GDPR's right to contestation.

1. *The Right to Be Forgotten.* — The "Right to Be Forgotten" (RTBF), more accurately characterized as a right to erasure of certain personal data, grew from European data protection law in existence before the GDPR.[393] In the 2014 *Google Spain* case, the Court of Justice of the European Union (CJEU) interpreted data protection law to hold that a search engine must, as a "data controller," respond to certain requests from individuals to erase personal data—that is, to challenges by individuals to the inclusion of their personal data in search engine results.[394]

391. Id. § 57(2)(b). France bans automated decision-making, including semi-automated decision-making, in the judicial context. Fully automated administrative decisions are also prohibited. However, semi-automated decisions are permissible in particular contexts, under conditions that include implementing administrative procedures for appeals. Malgieri, Automated Decision-Making in the EU Member States, supra note 115, at 13.

392. See supra note 387 and accompanying text.

393. The right emerged in current form from the Court of Justice of the EU's (CJEU's) 2014 case, *Google Spain*, and exists in current form in Article 17 of the GDPR. For a compelling history of its origins and characterization of its nature, see Meg Leta Ambrose & Jef Ausloos, The Right to Be Forgotten Across the Pond, 3 J. Info. Pol'y. 1, 6–11 (2013).

394. See Case C-131/12, Google Spain SL v. Agencia Espanola de Proteccion de Datos, ECLI:EU:C:2014:317, ¶ 100(3) (May 13, 2014).

The RTBF thus functions, in effect, as a right to contest inclusion in search engine results.[395] The RTBF is not an absolute right to erasure but rather a right to *request* erasure, with the search engine, as with the DMCA, acting both as an interested party and as arbiter. Unlike the DMCA, however, the RTBF contains no putback mechanism—and in fact, establishes virtually no procedural rules at all.[396]

The *Google Spain* decision was quickly characterized as a blow to free speech, with European authors noting that the CJEU failed to explicitly consider the fundamental right to freedom of expression.[397] Others identified the decision as a prime example of core differences between the U.S. and EU approaches to managing the tension between privacy and speech.[398] This focus on free speech, however, risks obfuscating the utility of the RTBF as a contestation model.

Among our contestation archetypes, the RTBF is most accurately characterized as a contestation standard with a substantive focus. The CJEU in *Google Spain* established substantive requirements for search engines to use in determining whether to delist search results. The court found that "as a rule" individual rights to data protection and privacy "override . . . not only the economic interest of the operator of the search engine but also the interest of the general public in having access to that information upon a search relating to the data subject's name."[399] But the court also established a substantive balancing test for search engines to use in establishing exceptions. Companies may balance between individual interests in privacy and data protection and a public interest in access to information.[400]

---

395. See Edward Lee, Recognizing Rights in Real Time: The Role of Google in the EU Right to Be Forgotten, 49 U.C. Davis L. Rev. 1017, 1037 (2016) (describing the process as an "administrative procedure for filing and deciding RTBF claims").

396. See id. at 1023 (noting that the CJEU left erasure requests to the discretion of the search engine or other entity receiving the request).

397. See Bloch-Wehba, supra note 293, at 52–56 (noting how "*Google Spain* and the Article 29 Working Party guidelines . . . chafe[] against free expression norms and values recognized in Europe and beyond"); Daphne Keller, The Right Tools: Europe's Intermediary Liability Laws and the EU 2016 General Data Protection Regulation, 33 Berkeley Tech. L.J. 287, 354 (2018) (discussing how the RTBF is both similar to and different from intermediary liability); Stefan Kulk & Frederik Zuiderveen Borgesius, *Google Spain v. González*: Did the Court Forget about Freedom of Expression?, 5 Eur. J. Risk Regul. 389, 397 (2014) (discussing the court's reliance on private ordering and observing that "search engine operator[s] may not be the most appropriate party" to balance the fundamental rights involved).

398. See, e.g., Steven C. Bennett, The "Right to Be Forgotten": Reconciling EU and US Perspectives, 30 Berkeley J. Int'l L. 161, 167–68 (2012); Orla Lynskey, Control Over Personal Data in a Digital Age: *Google Spain* v *AEPD and Mario Costeja Gonzalez*, 78 Mod. L. Rev. 522, 531 (2015); Robert C. Post, Data Privacy and Dignitary Privacy: *Google Spain*, the Right to be Forgotten, and the Construction of the Public Sphere, 67 Duke L.J. 981, 1061–62 (2018).

399. Case C-131/12, Google Spain SL v. Agencia Espanola de Proteccion de Datos, ECLI:EU:C:2014:317, ¶ 99 (May 13, 2014).

400. Id. ¶ 81.

Under certain circumstances, companies may maintain information in search results, for example when the individual is a public figure and the interest of the general public in such information outweighs privacy concerns.[401]

The CJEU's opinion in *Google Spain* establishes a contestation standard rather than a rule. It requires companies to respond to individual takedown requests, but leaves a great deal of leeway for determining what constitutes an individual interest in privacy and what constitutes a public interest in access to information.[402] What the CJEU did not do is give any indication of the procedure a search engine must follow: The CJEU decision emphasized substance, without establishing a contestation process.

Over time, both companies and regulators have filled in some of the gaps left by the CJEU. First, Google established an Advisory Council that issued a report indicating the substantive criteria the search engine would use in evaluating takedown requests.[403] Regulators then established their own list of criteria.[404] This dialogue has largely clarified the substantive standard set by the CJEU into something more rule-like in nature.

> Whilst it is true that the data subject's rights protected by those articles also override, as a general rule, that interest of internet users, that balance may however depend, in specific cases, on the nature of the information in question and its sensitivity for the data subject's private life and on the interest of the public in having that information, an interest which may vary, in particular, according to the role played by the data subject in public life.

Kulk & Borgesius, supra note 397, at 398.

401. Case C-131/12, Google Spain SL v. Agencia Espanola de Proteccion de Datos, ECLI:EU:C:2014:317, ¶ 97 (May 13, 2014) ("[T]he interference with his fundamental rights is justified by the preponderant interest of the general public in having . . . access to the information in question.").

402. See id. ¶ 81.

403. In the immediate aftermath of the court's decision, Google established an Advisory Council and went on tour, holding public meetings in seven European cities to discuss the substance of the right. Lee, supra note 395, at 1044. Google's Advisory Council issued a forty-one-page report in 2015, pointing to four substantive criteria: an individual's role in public life, the nature of the information, the source of the information, and the passage of time. The Advisory Council to Google on the Right to be Forgotten (Feb. 6, 2015), https://static.googleusercontent.com/media/archive.google.com/en//advisorycouncil/advisement/advisory-report.pdf [https://perma.cc/G5DJ-G7TG]; see also Paulan Korenhof, Jef Ausloos, Ivan Szekely, Meg Ambrose, Giovanni Sartor & Ronald Leenes, Timing the Right to be Forgotten: A Study Into "Time" as a Factor in Deciding About Retention or Erasure of Data, *in* Reforming European Data Protection Law 171, 172–73, 180–84 (Serge Gutwirth, Ronald Leenes & Paul de Hert eds., 2015) (exploring the role of time in the RTBF and identifying "specific points in data processing, which also denote specific points or periods in time, where enforcing of RTBF is reasonable or even necessary").

404. The Article 29 Working Party, the leading data protection regulator, issued guidelines in November 2014, with thirteen substantive criteria for balancing when to delist content. Article 29 Working Party, Guidelines on Google Spain, supra note 308. Once the GDPR went into effect, with a new provision specifically describing a right to erasure as a "right to be forgotten," the European Data Protection Board (EDPB) set about creating a new set of guidelines, adopted in July 2020. These Guidelines largely reference the previous

Regulators have not, however, set out a specific process that search engines must follow. In the absence of such rules, Google created its own process.[405] The RTBF has prodded companies into creating a privatized system of contestation similar to, but in some ways crucially different from, the DMCA. That system was likely influenced by implementations of the E-Commerce Directive, an EU-wide instrument established in 2000.[406]

Google set up what Edward Lee has described as an "administrative procedure for filing and deciding RTBF claims."[407] Google put a webform up on its website for individuals to request delisting.[408] The requester also had to provide a document verifying their identity and (as with the DMCA) attest to the accuracy of the representations made.[409] The current version of the webform is similar to what Lee describes but appears to contain some changes.[410]

At least initially, Google hired fewer than a hundred employees to process claims "on a case-by-case basis."[411] Sometimes the staff would reach

---

Guidelines under the Directive, delineating the substantive criteria that support a data subject's right to delisting, and exceptions to the right, following Article 17 of the GDPR. See GDPR, supra note 13, art. 17; European Data Protection Board, Guidelines 5/2019 on the Criteria of the Right to be Forgotten in the Search Engines Cases Under the GDPR (July 7, 2020), https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201905_rtbfsearchengines_afterpublicconsultation_en.pdf [https://perma.cc/8AH7-MKWQ] ("[T]he criteria of delisting developed by the Article 29 Working Party in guidelines on the implementation of the Court of Justice . . . C-131/12 can still be used by search engine providers and Supervisory Authorities to assess a delisting request based on the Right to object (Article 17.1.c GDPR).").

405. Lee, supra note 395, at 1037.

406. E-Commerce Directive, supra note 343.

407. Lee, supra note 395, at 1037.

408. Id. at 1038. Lee describes the webform at the time as containing the following fields: (1) which country's law applies; (2) personal information, including the name used to search; (3) the specific URLs desired removed, and an explanation as to (a) how the web page is related to the requester and (b) "how the inclusion of this URL as a search result is irrelevant, outdated, or otherwise objectionable." Id.

409. Id. at 1038–39.

410. It now requires: (1) the country of origin (similar to which country's law applies); (2) the full legal name and contact email address of the requester, and a statement of whether the requester is acting on their own behalf or someone else's; (3) specific URLs requested delisted (same as Lee describes). EU Privacy Removal: Personal Information Removal Request Form, Google, https://www.google.com/webmasters/tools/legal-removal-request?complaint_type=rtbf&visit_id=637202230061146146-20083139&rd=1 [https://perma.cc/2CLS-5YGJ] (last visited Aug. 2, 2021). However, the reason requested is changed to the arguably vaguer request for "(1) how the personal information identified . . . relates to the person on whose behalf th[e] request is made; and (2) why . . . the . . . information should be removed. For example: '(1) This page is about me because a, b, and c. (2) [It] should be removed because x, y, and z.'" Id. Under the current form, Google no longer indicates its criteria for delisting in its request for information from the individual. Id. The attestation requirement is still there, with an individual having to make a sworn statement as to accuracy. Id.

411. Lee, supra note 395, at 1039–40.

out to the requester for more information.[412] For harder cases, Google would rely on a self-created "senior . . . panel consisting of 'senior lawyers, engineers, and product managers,' " which would occasionally call in an outside expert.[413] If a claim was rejected, Google sent a rejection indicating reasons and pointing to the complainant's right to file a complaint with a national data protection authority.[414] If Google found the claim valid, it notified the requester of removal of the URL.[415]

As mentioned, the primary criticism of the RTBF is that it skews toward delisting.[416] Webmasters have limited options to ask for relisting;[417] members of the general public have no way to state an interest in keeping information searchable.[418] Commentators have criticized the reliance on private companies to balance what in the EU are fundamental rights.[419] Unless companies voluntarily disclose information, there is no window into the decision-making process.[420]

Perhaps surprisingly, however, the RTBF did not, as some naysayers predicted, break the internet in Europe.[421] Google established a process for handling complaints that appears to be manageable, at least for that company.[422] Google's transparency reports indicate that roughly fifty-eight

412. Id. at 1040.

413. Id. (quoting Lisa Fleisher & Sam Schechner, How Google's Top Minds Decide What to Forget, Wall St. J. (May 12, 2015), https://www.wsj.com/articles/how-googles-top-minds-decide-what-to-forget-1431462018 (on file with the *Columbia Law Review*)).

414. Id. at 1040–41.

415. Id. at 1041 ("If the claim for removal is accepted, Google sends the requester a notice indicating the removal of the URL.").

416. See Kulk & Borgesius, supra note 397, at 394–95 (noting that the *Google Spain* judgment resembles intermediary liability under the E-Commerce Directive, which "creates an incentive for intermediaries to systematically take down content after complaints, which may interfere with the freedom of expression of those communicating on the internet").

417. Id. at 396–97 ("If Google delists a search result, it informs the relevant website publisher. Google tells the website publisher which URL it delisted, but does not disclose who submitted the request or other details about the request . . . . [T]he publisher can ask Google to re-evaluate the delisting.").

418. Id. at 397 (explaining that Google's practice leaves the public with no way to oversee how their right to access information is limited).

419. Id. at 394 (discussing the court's reliance on private ordering and observing that "search engine operators may not be the most appropriate party to balance the fundamental rights involved").

420. See id. at 395 ("A general problem of private ordering by online service providers through notice and takedown mechanisms is the lack of transparency of their decisions.").

421. See Robert Krulwich, Opinion, Is the 'Right to Be Forgotten' the 'Biggest Threat to Free Speech on the Internet'?, NPR (Feb. 24, 2012), https://www.npr.org/sections/krulwich/2012/02/23/147289169/is-the-right-to-be-forgotten-the-biggest-threat-to-free-speech-on-the-internet?t=1627911057362/ [https://perma.cc/M9V9-7NZD] (suggesting that internet companies may delist content quickly to avoid fines or criminal prosecution, inhibiting the public's right to know and freedom of the press).

422. See Lee, supra note 395, at 1038–41.

percent of targeted content stays up.[423] Still, there are costs to leaving substantive discretion to private companies and costs to failing to articulate processes in detail.[424] Certain interests, such as the public's, are left out of the process.[425] The process and substance of decisions can appear less legitimate.[426] And while Google has established procedures that seem to largely, though not entirely, map onto other familiar contestation mechanisms, other, smaller companies might not have the desire or capacity to adopt the same.

2. *The Hungarian and Slovenian Implementations of the GDPR's Right to Contestation.* — Several EU Member States have established substantive backstops to the GDPR's right to contestation.[427] For example, Hungary requires that automated decision-making "not infringe the requirement of equal treatment."[428] Slovenia states that decisions "based on the processing of particular categories of personal data . . . are . . . prohibited if they could lead to discrimination against the data subject or persons close to her/him."[429] Slovenia identifies the right to contest as a measure "for protecting human rights and fundamental freedoms and the legitimate interests of the individual."[430]

Slovenia and Hungary thus each anchor their contestation schemes to a substantive standard rather than a rule. Creating a backstop based on fundamental rights of nondiscrimination and equal treatment arguably preserves dignitary interests. It also reduces the risk that the Slovenian and Hungarian schemes decay into empty processes untethered from substance, as has happened with, for example, some implementations of the DMCA.[431]

At the same time, this approach creates interpretative space, which has both costs and benefits. What constitutes "discrimination" or "equal treatment" is hotly contested.[432] On the one hand, this creates flexibility for applying the right in new contexts. On the other, it potentially leaves leeway for less stringent implementations by self-interested actors. We advocate in

423. Id. at 1043.

424. See, e.g., Kulk & Borgesius, supra note 397, at 393 (explaining that delisting information conflicts with freedom of expression).

425. Id.

426. See id. at 395 ("A general problem of companies [delisting] . . . through notice and takedown mechanisms is the lack of transparency of their decisions. Without clarity on which results have been delisted, members of the public have limited ability to know the extent to which their freedom to receive information has been interfered with.").

427. Malgieri, Automated Decision-Making in the EU Member States, supra note 115, at 2.

428. Id. at 16.

429. Id. at 18.

430. Id.

431. See supra section III.C.1.

432. See Barocas & Selbst, Big Data's Disparate Impact, supra note 70, at 715.

Part IV below for ways to constrain self-interested interpretations of substantive backstops, to preserve the utility of a substantive standard without sacrificing some of the benefits that come with the constraints that typify rules.

E. *Archetype 4 Illustrated: The FCBA's Chargeback Process and the Hungarian and French Rights to Contestation*

Our fourth and final contestation archetype is a *contestation rule* with a *substantive focus*. This example, the 1974 FCBA, is not intrinsically digital, but it still holds lessons for the right to contest AI.[433] Components of the French and Hungarian implementations of the GDPR's right to contestation also illustrate this archetype.

1. *The Fair Credit Billing Act.* — The FCBA affords consumers a right to contest erroneous credit card charges.[434] In many ways, the FCBA is structurally similar to section 512 of the DMCA. First, it provides the substantive basis of contestation. The law defines a contestable "billing error" to include: a charge that wasn't made by the credit card holder; a charge that is in the wrong amount; a charge for which the credit card holder requests additional clarification; a charge for goods or services that weren't accepted or delivered; accounting errors; and more, including errors defined by regulation.[435] Second, in addition to the substantive definition of "billing error," the law contains various detailed procedural requirements.[436] And, as with each of the archetype examples, there is no neutral arbiter in the FCBA process. Credit card companies themselves decide whether or not to reverse charges.[437]

Yet the FCBA does not founder in empty proceduralism as some implementations of the DMCA do. Rather, it retains its substantive focus while providing detailed process requirements.[438] This is likely for a few reasons. First, the substantive clarity of the statute constrains credit card companies' discretion to reject reversal requests. The extensive, specific substantive definition of a "billing error" tethers credit card companies' discretion in the contestation process.[439] By contrast, the DMCA ties takedown to copyright infringement[440]—still substantive, still rule-based, but much more complicated to determine (and contestable) than whether an FCBA "billing error" has occurred. Second, while both models rely heavily on precisely defined processes, differences in the design of those

433. See Van Loo, supra note 5, at 851–52 (identifying the relevance of credit card dispute adjudications to the conversation over platform process).

434. 15 U.S.C. § 1666 (2018).

435. Id.

436. Id. § 1666(a); 12 C.F.R. § 226.13(d) (2020).

437. See Van Loo, supra note 5, at 852.

438. See 15 U.S.C. §§ 1666(a)–(b).

439. However, federal courts have refused to second-guess companies. Section III.F below discusses this wrinkle further. See Burnstein v. Saks Fifth Ave. & Co., 208 F. Supp. 2d 765, 775 (E.D. Mich. 2002).

440. See 17 U.S.C. § 512(c)(1) (2018).

processes create different incentives, risk structures, and, ultimately, outcomes.[441] These differences, and their effects, are discussed further in Part IV.

In practice, the FCBA appears to be quite successful in resolving billing disputes and enjoys a more positive reputation than the DMCA.[442] As Rory Van Loo notes, the FCBA establishes a working contestation process that is "free, accessible, and fast" and has not "necessarily come at the expense of merchants."[443] Credit card companies have benefited, too, from increased consumer trust fostered by the FCBA contestation process.[444] Scholars of alternative dispute resolution have criticized the FCBA process on a number of grounds, including the lack of damages, limited consumer awareness of the process, and the arms-length rather than relationship-based method of adjudication.[445] Consumer protection advocates, however, largely see the FCBA chargeback process as a success.[446] Credit card companies rule in favor of consumers some eighty to ninety percent of the time.[447] Perhaps because of this rate of success, consumers appear to view the process with satisfaction, and rarely bring suits to challenge it.[448]

This is not to say that the FCBA is a perfect model or that it can necessarily be replicated for every kind of dispute. For example, the FCBA may be successful in part because its substantive scope *can* be clearly defined. It is far easier to define an erroneous credit card charge than to define copyright infringement or discrimination.[449] And there can be costs to a constrained, ex ante definition of the substance of challenges, including limiting the scope of contestation and missing newly developed problems as technology evolves. But as recent conversations about the use of personal data have turned to the centrality of consumer trust, policymakers might do well to look to the FCBA as a contestation model.[450]

---

441. See generally 15 U.S.C. § 1666; 17 U.S.C. § 512 (presenting the procedural and substantive requirements under the DMCA and FCBA and the overall framework of the acts).

442. See Van Loo, supra note 5, at 854, 859.

443. Id. at 854.

444. Id.

445. Id. at 853 (citing Amy J. Schmitz, There's an "App" for That: Developing Online Dispute Resolution to Empower Economic Development, 32 Notre Dame J.L. Ethics & Pub. Pol'y 1, 16–19 (2018)).

446. See Van Loo, supra note 5, at 853 (citing Henry H. Perritt, Jr., Dispute Resolution in Cyberspace: Demand for New Forms of ADR, 15 Ohio St. J. on Disp. Resol. 675, 691 (2000)).

447. See Van Loo, supra note 5, at 854.

448. See id. at 853.

449. Section IV.A below discusses this further.

450. Ari Ezra Waldman, Privacy as Trust: Information Privacy for an Information Age 61 (2018) (discussing what trust means for privacy); Neil Richards & Woodrow Hartzog, Taking Trust Seriously in Privacy Law, 19 Stan. Tech. L. Rev. 431, 451 (2016) ("Because disclosure of personal data leaves people vulnerable, trust is the glue that holds together virtually every information relationship.").

2. *The Hungarian and French Implementations of the GDPR's Right to Contestation.* — Both the Hungarian and French implementations of the GDPR's right to contestation contain contestation rules with a substantive focus. Hungary requires that automated decision-making not be "made using sensitive data, unless otherwise provided for in the law."[451] France similarly prohibits automated decision-making based on sensitive data.[452] An individual contesting a particular decision could refer to these prohibitions. If a company's decision-making violates them, presumably the company would be required to reverse its decision.

Again, however, these are not perfect instantiations of the archetype. The substance of France's law is embedded within a deeply procedural administrative law framework, as section III.D discusses above. Hungary also includes, in addition to its substantive rule, the broad substantive standard ("the requirement of equal treatment") discussed above in section III.D.

F. *The Design of Privatized Process: Other Considerations*

In addition to the two key axes illustrated by the four archetypes, contestation schemes may vary in other important characteristics. These also can affect the schemes' ability to provide meaningful process and should be taken into account when designing and operationalizing a contestation right. First, there is the question of who decides. A contestation scheme may house contestation with a neutral arbiter, have a mediating platform adjudicate, or have one of the parties themselves adjudicate. Second, how contestation schemes structure parties' incentives matters. Third, transparency matters. Subjecting decisions to public transparency over time—a core element of judicial process—can illustrate whether a contestation scheme is systemically fair. Finally, contestation schemes are heavily affected by the details of the regulatory context in which they reside. For example, contestation can be a stand-alone right, or it can be housed within a broader regulatory system that also provides systemic governance tools.[453] For example, the GDPR's right to contestation is just one element of the GDPR's approach to algorithmic accountability. The GDPR also deploys a number of systemic regulatory tools, for example impact assessments,[454] which act as risk mitigation processes. Companies also have reporting and recording obligations[455] and obligations to design technology to protect individual rights.[456] Each of these governance tools aims to

451. Malgieri, Automated Decision-Making in the EU Member States, supra note 115, at 16.

452. Id. at 13.

453. See Kaminski, Binary Governance, supra note 12, at 1578 ("Individual rights can produce instrumental contributions, be an important component of systemic accountability, [and] give substance to the rules in a collaborative governance regime . . . .").

454. See Kaminski & Malgieri, Impact Assessments, supra note 287.

455. GDPR, supra note 13, art. 30.

456. Id. art. 25.

correct errors and protect from bias and discrimination on a systemic scale, complementing individual rights.

Context also includes other elements of regulatory setting and regulatory design. Even where a contestation scheme is largely privatized, it often interacts with a background regulatory environment that can be calibrated to check privatized contestation. A contestation scheme may, like the DMCA, have a judicial backstop that enables sanctions of parties who misrepresent the substantive law.[457] It may be set within a complex regulatory scheme with significant penalties, such as the GDPR, in which regulators are armed with large fines and a human rights court may be willing to intervene.[458] Or, as with the FCBA, federal courts may refuse to intervene in second-guessing parties' decisions.[459] Background rights may favor one party or the other, depending on the rights implicated (for example, copyright, free speech, or privacy) and on the legal system of the country in which the contestation scheme has been structured. Background rights, too, can be legislative in nature or constitutional/fundamental, varying the kinds of interventions courts or regulators might make.

IV. CRAFTING A MEANINGFUL RIGHT TO CONTEST AI

No matter how strong the case for a right to contest AI, it will fail if not carefully designed and implemented. Contestation schemes can fail to fulfill due process values or actually undermine them, losing legitimacy. Or they can fail because they simply don't work: They are too costly to invoke, they are too difficult to use, or they don't resolve the dispute. This final Part considers how to design an effective right to contest AI—one that resolves disputes, meets due process goals, and is seen as legitimate.

There is no one right way to design a right to contest AI. Legislators could take any one of the archetypes as a starting point and adjust it to avoid foreseeable pitfalls. Moreover, contestation is contextual and entangled with other aspects of process such as notice and reason giving, the specifics of underlying substantive law, and incentive structures. Designing a successful contestation mechanism requires attention not just to contestation itself, and not just to the algorithm, but to the *entire decision-making system—human, machine, and organizational*—together with the underlying legal framework.

The complexities of contestation thus do not neatly lend themselves to a one-size-fits-all prescription. However, there are better and worse ways to design contestation, with significant lessons to be learned from both the theory and case studies explored above. This Part analyzes the observations, archetypes, and case studies from Part III, placing them against the

457. 17 U.S.C. § 512(f) (2018).

458. GDPR, supra note 13, ch. 8.

459. See, e.g., Burnstein v. Saks Fifth Ave. & Co., 208 F. Supp. 2d 765, 775 (E.D. Mich. 2002).

due process values set forth in Part II to draw practicable lessons about the design and implementation of this right.

We begin with the archetypes from Part III. While a right to contest AI could track any of the archetypes, the case studies illustrate how best to avoid design pitfalls. This Part then turns to privatized process design, including how to craft participation, the role of the decision-maker, risks and incentive structures, and the importance of regulatory context and of systemic governance and transparency. It then explains that the right to contest AI should constitute a floor, not a ceiling, which might be augmented in certain policy settings. This Part concludes by discussing coverage thresholds and possible exceptions and challenges.

A. *Applying the Archetypes*

Part II details the theoretical goals of an individual right to contest: improving accuracy and reducing bias, supporting rule of law values such as consistency and rationality, and affording respect and agency to individuals. Each contestation archetype Part III describes has strengths and weaknesses with respect to these due process goals and values.

A right to contest AI that, like the GDPR's Article 22, tracks the archetype of a *contestation standard* with a *procedural focus* raises several problems.[460] Failing to clarify a substantive basis for contestation potentially allows self-interested decision-makers to defang the right, making it useless in practice. If there is no clear and consistent substantive basis for challenges, individual challenges are unlikely to serve the instrumental function of improving accuracy or preventing bias. Nor are individual challenges likely to serve rule of law values if there is no common substantive standard under which decisions could be evaluated for consistency.

With respect to dignity, affording individual challenges with no clear substantive basis or set of procedures could make it harder for individuals to exercise agency or feel respected by the system. The lack of procedural clarity in a contestation standard (versus a rule) risks disempowering individuals, rather than affording them a clear avenue for process. At best, a contestation standard with a procedural focus imposes on decision-makers the significant costs of determining when decisions should be overturned and of establishing sufficiently clear and meaningful process for affected individuals to feel respected by the system.

A right to contest that, like the UK's implementation, illustrates a *contestation rule* with a *procedural focus* faces similar problems. It too risks overproceduralizing at the expense of substance, undermining due process values such as accuracy and rule of law. By providing clear procedural rules and timelines, however, it potentially puts contestation within the reach of more individuals, giving more people a sense of agency by lowering the information costs of contesting decisions. The efficacy or legitimacy of

460. See supra Part III.

such a system depends on how well-meaning decision-makers are, what sorts of substantive challenges are considered, how consistent substance is across challengers, and more broadly, what incentives decision-makers have to decide for or against challengers.

Affording a right to contest with a clear substantive focus, whether rule-based or standard-based, can address a number of these concerns. However, the right to challenge a decision on substantive grounds can still be meaningless if the afforded process is shallow or perfunctory. For example, if a contestation process has no clear timelines, decision-makers can delay challenges, stymieing multiple due process goals: corrections of inaccuracies, revelations of unfair or inconsistent treatment, empowerment of individuals. Other missing particulars of process can similarly shift a right to contest from substantive to illusory. Without clear notice, a person won't know to challenge an unfair decision. Similarly, if there is no reason giving, individuals will find it difficult or impossible to challenge an AI decision on the basis of a substantive problem, as section IV.B discusses further below.

As discussed above, contestation rights with a substantive focus can present additional issues depending on how legislators have defined the substantive bases of challenges. A right to contest that, like the Hungarian implementation, illustrates a *contestation rule* with a *substantive focus* risks on the one hand being overbroad, banning all automated decisions based on particularly sensitive data, whether or not such decisions are inaccurate or unbiased or unfair. On the other hand, a rule with a substantive focus risks being too narrow, missing challenges individuals should be able to bring. However, a right to contest that, like the Slovenian implementation, embodies a *contestation standard* with a *substantive focus* risks instead creating too much leeway for substantive interpretation, imposing costs on both challengers and decision-makers. There is no one definition of discrimination, and delegating the interpretation of discrimination to private companies risks both confusion and self-serving interpretations.

However, understanding the archetypes and the pitfalls they present can help legislators and regulators avoid many of these pitfalls, not just in enacting new laws but in applying those that now exist. For example, where the GDPR largely articulates a standard with a procedural focus, regulators and Member States should now focus on (1) creating more detailed timelines and processes to standardize the required procedure, and (2) articulating more clearly the substantive harms on which such challenges might be based, even if this involves pointing to other substantive areas of EU or Member State law.[461] Member States that have implemented the right through a different archetype could focus their efforts differently. Regula-

461. See supra note 129 (explaining that while Article 22 is procedural in nature, other substantive areas of EU law can be understood to give it substance).

tors in Slovenia, for example, might establish a workable contestation process and timeline, while regulators in Ireland might establish or point to substantive bases for contestation.

For countries that have not yet enacted a right to contest AI, a hybrid approach is advisable—that is, a law that contains elements of multiple archetypes and uses multiple regulatory tools. A right to contest that combines clear procedural rules with both substantive rules and substantive standards is the better path forward as a starting point than reflexively mimicking either the GDPR or the DMCA/UK approach.

The FCBA model—a *contestation rule* with a *substantive focus*, where the substantive underpinnings are clear and relatively straightforward to apply—potentially has significant benefits, as section III.E discusses above. However, determining what constitutes AI bias is far harder to determine than what constitutes an erroneous credit card charge. The right to contest AI could then be partially modeled after the FCBA archetype, with some clear substantive rules: that an AI decision cannot be made on the basis of racial data, or gender, or sexual orientation, for example, because such decisions are de facto biased.

Coupling a set of specific substantive rules with a contestation standard has the benefit of being simultaneously clear and flexible. With the archetypes in mind, regulators could adopt a standard—for example, that establishes a right to contest AI decisions that evidence "bias" or "discrimination"—while also avoiding the foreseeable pitfalls of standards. A variety of common drafting or regulatory tools can help. For example, legislators or regulators can clarify standards without forgoing malleability by providing an open list of examples. Regulators can issue soft law guidance. Legislators or regulators could bring in external participation and accountability, requiring companies to consult affected stakeholders and legal experts when defining what "bias" and "discrimination" mean in a particular context.[462] Legislators might establish certification processes or codes of conduct backed by regulatory oversight, as the GDPR does, to give substance to standards in sectoral context. Ex post, courts could articulate substantive backstops, for example by affording an avenue for legal challenges to AI decision-making after an individual exhausts a privatized contestation right.[463]

In sum, while a contestation right is unlikely to succeed or fail solely because it is based on a particular archetype, due process goals are better served with certain common features. Clear process can make it easier for

462. This once again points to the importance of embedding an individual right to contest in a broader regulatory scheme, as the GDPR does, and as Slovenia does in particular.

463. Some have suggested not only allowing court challenges to discriminatory AI decision-making but also placing a burden on a company to prove the system is not discriminatory. Ifeoma Ajunwa, Paradox of Automation, supra note 4, at 1726 (proposing a doctrine of "discrimination per se" if employers fail to audit or otherwise quality check algorithms); James Grimmelmann & Daniel Westreich, Incomprehensible Discrimination, 7 Calif. L. Rev. Online 164, 170 (2017).

individuals to contest AI decisions, giving them a sense of agency and bolstering the perceived legitimacy of a system. Clear substance can direct challenges appropriately, lower costs of participation, and better serve specific instrumental goals, such as accuracy or antidiscrimination. Both clear process and clear substance can serve rule of law values by uncovering arbitrariness, unfairness, or irrational decision-making. However, there is also value in flexibility, particularly with regard to substance, as it can accommodate previously unanticipated goals or values and support stakeholder and expert participation.

B. *The Right to Contest as Privatized Process: Notice and a Hearing*

However well-crafted a right to contest AI, individual participation can be illusory if it is not supported by certain features. Participation rights should feature familiar elements of due process: notice, reason giving, and an opportunity to be heard before a legitimate, if not neutral, decision-maker.[464] They should also include design elements beyond due process, such as incentive structures that support legitimate decision-making and recognition of the broader regulatory context, including backing individual challenges with robust systemic governance.

1. *Meaningful Notice and an Opportunity to Be Heard.* — The paradigmatic elements of due process as articulated by Judge Henry Friendly include: notice of a decision and the grounds of that decision, a right to know the evidence on which a decision is based, a hearing before an unbiased decision-maker or tribunal, a right to present arguments against a decision; and a statement of reasons.[465] Friendly's elements are more of a menu than a checklist; what constitutes a fair hearing may vary with circumstances such as the level of harm and administrative costs.[466]

It would be challenging to administer a number of Friendly's elements in the context of a right to contest AI.[467] However, a right to contest AI that does not include at least elements of notice, evidentiary disclosure, and reason giving will not provide a meaningful hearing. Individuals cannot correct inaccurate decisions if they cannot see the incorrect data, reasoning, or inferences underlying decisions. Individuals cannot be assured that decision-making is being applied nonarbitrarily if they cannot understand a decision-making system's logic. And individuals are unlikely to feel respected by a contestation right that does not provide a sufficient window

---

464. See Friendly, supra note 2, at 1279–95 (advocating for notice of the proposed action and grounds asserted, right to know the evidence, and statement of reasons).

465. Id. at 1279, 1280–81, 1283–87, 1291–92; see also Crawford & Schultz, supra note 8, at 116 (summarizing Friendly's eleven elements of a fair hearing).

466. Friendly, supra note 2, at 1278.

467. Crawford & Schultz, supra note 8, at 116, noting that administering a right to call witnesses in the context of "data due process" would be "difficult and potentially cumbersome." Of Friendly's elements, they point to "an unbiased tribunal," "the right to know the evidence against one," "the making of a record," and "a statement of reasons" in the data analytics context. Id. at 117.

into decision-making—through notice, evidence, and reason giving—to make meaningful challenges possible.

The GDPR's transparency requirements reflect longstanding due process traditions and are intended to enable the contestation right.[468] The GDPR requires that individuals be notified when a decision involves automated decision-making.[469] The GDPR's general rights to review and correct data can provide data subjects with information on which to base a challenge.[470]

In the context of AI decision-making, however, notice and access rights are not enough. Due process theory explains that reason giving plays a central role.[471] Friendly describes reason giving as necessary for a number of purposes: to prevent wrong decisions, to achieve more uniformity across decisions, and to make negative decisions more acceptable.[472] Frederick Schauer similarly describes reason giving as displaying commitment to an outcome, allowing decision disciplining, and showing respect for the subjects of decisions.[473] For a right to contest AI decisions to be effective, individuals must be afforded access to both the AI's "record" and its reasoning.

The GDPR consequently requires both that individuals affected by AI decision-making be provided "meaningful information about the logic involved" in such decision-making,[474] "the significance and envisaged consequences" of the decision-making process,[475] and a "right to explanation."[476] The GDPR's much-debated "right to explanation" requires that individuals be provided an explanation of automated decisions with significant effects.[477] What this constitutes has been hotly debated.[478] EU Member States

468. See supra section III.A.

469. GDPR, supra note 13, arts. 13(2)(f), 14(2)(g).

470. All of this information must be given in "a concise, transparent, intelligible and easily accessible form, using clear and plain language" in the form requested by the data subject. GDPR, supra note 13, art. 12(1).

471. Margot E. Kaminski, Understanding Transparency in Algorithmic Accountability, *in* The Cambridge Handbook of the Law of Algorithms 121, 128–29 (Woodrow Barfield ed., 2020) ("Transparency takes many different shapes and sizes . . . . [A] person impacted by a lending decision might be provided an explanation of that decision, at an abstract enough and simple enough level so as to be understandable, but also complex enough to be actionable, to allow her to contest the decision.").

472. Friendly, supra note 2, at 1292.

473. Schauer, Giving Reasons, supra note 207, at 657–58.

474. GDPR, supra note 13, arts. 13(2)(f), 14(2)(g). There is some debate over whether "meaningful information about the logic involved" refers to a particular decision or to an overview of how the AI works as a whole. Wachter et al., Counterfactual Explanations Without Opening the Black Box, supra note 27, at 860 n.69; Selbst & Powles, supra note 127, at 241 n.41.

475. GDPR, supra note 13, arts. 13(2)(f), 14(2)(g).

476. Id. art. 13(2).

477. Kaminski, Right to Explanation, Explained, supra note 25, at 197.

478. Id. at 200.

have implemented the right to explanation in a variety of ways, ranging from France's requirement that decisions be "legible," to the UK's more minimalist interpretation.[479]

The GDPR is not alone in requiring reason giving and records. The FCBA similarly requires that a credit card company explain why it has failed to refund a charge and provide documentary evidence to support this reasoning on request.[480] By contrast, the RTBF does not mandate explanation of search engine decisions, although Google has voluntarily taken it upon itself to provide an explanation when it rejects a claim.[481] For a right to contest to be meaningful, there must be some individually comprehensible explanation of the reasoning behind a decision.

Other elements of a fair hearing include participation, such as an opportunity to explain why a decision is wrong or a right to call witnesses.[482] The GDPR's Article 22 includes at least two participation rights: a right to human intervention, and a right to "express his or her point of view."[483] These rights are interdependent with the GDPR's transparency rights and the particulars of how a contestation process is implemented. Whether a right to express one's point of view is meaningful will depend on whether the right to explanation provides a sufficient measure of reason giving to support meaningful participation. It will depend on whether the contestation process and timeline are clear and low cost. And it will depend on whether the substantive aspects of the decision, such as underlying law, are easily understandable. Proprietary algorithms and datasets only add impenetrability.[484]

It is unclear how robustly the GDPR's participation requirements will be incorporated into actual contestation procedures. This, again, suggests an advantage to contestation rules rather than standards. The highly proceduralized UK rubric allows the data subject to provide "additional information." It is unclear, however, what "additional information" can be provided, or how it will be treated. Depending on how it is operationalized, this could create robust participation, or instead result in very limited "conversations" that are unlikely to serve as a true "sign of respect" for the data subject.[485]

---

479. Malgieri, Automated Decision-Making in the EU Member States, supra note 115, at 14.

480. 15 U.S.C. § 1666(a)(3)(B)(ii) (2018) ("[S]end a written explanation or clarification to the obligor, after . . . an investigation, setting forth . . . the reasons why the creditor believes the account of the obligor was correctly shown in the statement and, upon request of the obligor, provide copies of documentary evidence of the obligor's indebtedness.").

481. Lee, supra note 395, at 1040–41.

482. Friendly, supra note 2, at 1281–82.

483. GDPR, supra note 13, art. 22(3).

484. See, e.g., Crawford & Schultz, supra note 8; Perel & Elkin-Koren, supra note 159, at 49.

485. Schauer, Giving Reasons, supra note 206, at 658, and accompanying text.

The French approach to the use of AI in the public sector demonstrates another way to structure a combination of reason giving and participation rights. French law requires not just reason giving but comprehensibility. In France, the law, at least as it applies to the public sector, requires the users of algorithms (that is, public officials) to be able to exercise control over them and to explain how they work to an affected person.[486] This is connected to robust participation rights: For public sector decisions, the "structured mechanism" for a right to contest AI is dictated by French administrative law, including robust administrative procedures.[487]

The French approach thus combines reason giving with human oversight, so as to create the possibility of meaningful intervention by the contesting parties and by the human using the algorithm.[488] Whether contestation should require such a level of human intervention and oversight capacity remains an open question. Such comprehensibility requirements could protect data subjects but will likely preclude the use of certain kinds of complex algorithms.

2. *A Legitimate Decision-Maker.* — A neutral arbiter is considered core to due process.[489] A neutral arbiter affords dignity to participants, tethers parties' discretion, and helps identify and eschew bias and error, ultimately providing confidence that decisions are accurate and fair. Schemes that lack a neutral arbiter may gain efficiency at the cost of legitimacy.

For example, one of the criticisms of the DMCA's notice-and-takedown process is that online platforms—chosen for their handy intermediary location between copyright holders and alleged infringers—are not neutral arbiters. Platforms' interests—in avoiding liability, attracting and keeping a user base, and limiting administrative costs—may be at odds with the disputants' interests. Neutrality concerns also pervade recent discussions of content moderation, with Facebook establishing the purportedly neutral Facebook Oversight Board to decide appeals.[490] There may be merit in a hybrid system in which initial arbiters are not necessarily neutral

---

486. French law requires that public authorities be able to exercise a mastery, or ensure control, over algorithmic decision-making to the extent of being able to explain, intelligibly and in detail, how the processing works to the impacted person (a loose translation of French law). *Pour ces décisions, le responsable de traitement s'assure de la maîtrise du traitement algorithmique et de ses évolutions afin de pouvoir expliquer, en détail et sous une forme intelligible, à la personne concernée la manière dont le traitement a été mis en oeuvre à son égard.* Malgieri translates this as "the data controller ensures the control of the algorithmic processing and its evolutions in order to be able to explain, in detail and in an intelligible form, to the person concerned how the processing has been implemented in his or her individual case." Malgieri, Automated Decision-Making in the EU Member States, supra note 115, at 13 (emphasis omitted).

487. Id.

488. Malgieri refers to this and other French law regarding private processing as "one of the few cases in which a law guarantees a right to explanation." Id. at 15.

489. Borraccetti, supra note 91, at 105.

490. Klonick, supra note 314.

but those who review their decisions are. Van Loo has suggested one such scheme by which privatized contestation overseen by companies can later be appealed to federal courts.[491]

In an ideal world, an uninvolved party would adjudicate contestation of AI decisions. In some settings, this may be possible, particularly where the potential harms to an affected person are high enough to justify the attendant administrative costs. For example, when AI is used in the criminal justice system, affected defendants should be afforded the ability to meaningfully contest AI decisions before a judge.[492] When AI decision-making is used in a regulatory setting, constitutional due process may require adjudication by a neutral party.[493]

A right to contest private sector AI decisions, however, is unlikely to include a neutral arbiter, at least at first bite. The privatized contestation schemes discussed in Part III illustrate this as a practical matter. Where speed and scale are concerns and the impact of decisions arguably less significant, the cost of a neutral arbiter can be prohibitive. Neither our archetype contestation schemes nor Article 22 feature a neutral arbiter. To the contrary, interested actors make the decisions.

Under Article 22, a company that uses AI to make decisions about a person will likely also be the arbiter of challenges to those decisions. At first glance, this might appear to delegitimize the entire process. However, as the next section discusses, setting up the right incentives for a nonneutral decision-maker can improve both outcomes and legitimacy. Jurisdictions that have not yet formulated a right to contest AI might consider balancing neutrality with efficiency, for example, by requiring the arbiter to hold an independent position within a company or by contemplating hybrid private–public systems for "appeals."

In some cases, the question isn't only whether there should be a neutral human decision-maker but whether there should be a human decision-maker at all. A contestation scheme can be entirely automated.[494] Some parties may be tempted to address the decision-maker cost and efficiency problem by replacing, or augmenting, human decision-makers with

491. Van Loo, supra note 5, at 871–72.

492. See, e.g., Roth, supra note 79, at 2039–51 (discussing the right to confront and impeach machine "witnesses"); Wexler, supra note 6, at 1395–413 (arguing against using a criminal trade secret privilege to prevent criminal defendants from examining and challenging software programs).

493. See, e.g., Huq, Constitutional Rights in the Machine-Learning State, supra note 8, at 1905–06. It is beyond the scope of this Article to discuss what meaningful contestation might entail in these contexts. It would certainly entail more than attaching a warning to AI tools as, for example, the Wisconsin Supreme Court has done. State v. Loomis, 881 N.W.2d 749 (Wis. 2016).

494. Urban et al., Notice and Takedown in Everyday Practice, supra note 287, at 29. Confronted with internet-scale infringement, some rights holders deploy algorithms to identify potentially infringing materials and generate notices. For the subset of OSPs that receive these notices—which can exceed a billion a year—the response is to automate the takedown process. One of us has called this system "DMCA Auto" and "DMCA Plus." Id.

AI.[495] Having an AI "judge" contestation "cases" would certainly make the system faster and less expensive.

However, having an AI arbiter would compound the difficulty of uncovering AI bias. Arbitrating AIs will have biases of their own—biases that may be difficult for humans to observe or understand. The GDPR places importance on recourse to a human, rather than AI, intervention in an AI decision. There is an active scholarly debate over the importance and effect more generally of having a "human in the loop."[496]

Where decision-makers aren't neutral arbiters, a privatized contestation system must tether decision-maker self-interest. One way to do so is to establish a judicial or regulatory backstop. Contestation could be appealable to a judge or neutral external board;[497] one could establish regulatory oversight over contestation systems;[498] or one could make abuse or misrepresentations legally actionable.[499] As the DMCA shows, however, none of these approaches is perfect; a legitimate contestation system might require multiple checks. Regulators might additionally require decisions to be made or overseen by an independent officer within a company, require reporting by a company to a regulator, or provide whistleblower protections for employees who wish to report on a contestation system. Section IV.B.4 further discusses such systemic regulations.

3. *Risk and Incentive Structures*. — The effects of a contestation scheme are deeply influenced by the incentive structures created by law and reflected in practice. Another way to tether decision-maker discretion is to structure decision-maker incentives such that even nonneutral decision-makers find it attractive to pursue accuracy and legitimacy, and to rule in favor of contesting individuals when appropriate. For example, the FCBA chargeback process encourages credit card companies to rule for challengers and refund charges, because the alternative—conducting an investigation—is expensive.[500] The UK's proceduralized implementation of the right to contest might similarly encourage companies to decide for individuals. By contrast, both the RTBF and section 512 processes operate in the shadow of liability risk for the online intermediaries making removal

495. See generally Huq, Constitutional Rights in the Machine-Learning State, supra note 8; Van Loo, supra note 5.

496. See, e.g., Huq, A Right to a Human Decision, supra note 8, at 681; Meg Leta Jones, The Ironies of Automation Law: Tying Policy Knots with Fair Automation Practices Principles, 18 Vand. J. Ent. & Tech. L. 77, 134 (2015); Rebecca Crootof, Margot Kaminski & Nicholson Price, Humans in the Loop 4 (unpublished manuscript) (on file with the *Columbia Law Review*).

497. See, e.g., Klonick, supra note 314, at 2425; Lee, supra note 395, at 1036; Van Loo, supra note 5, at 870.

498. See, e.g., Crawford & Schultz, supra note 8, at 109.

499. See 17 U.S.C. § 512(f) (2018).

500. Van Loo, supra note 5, at 854.

decisions. Consequently, both the DMCA and RTBF are criticized for skewing platforms' incentives toward removal.[501]

Incentives for contesting individuals also merit attention. For example, uneven legal requirements, resulting in uneven risk allocation, afflict the DMCA's complaint and contestation processes. Senders of takedown notices have to declare under penalty of perjury that they are authorized to act. However, none of senders' other statements, including their substantive assertions of infringement, is subject to this stricture.[502] But counternotice senders must accept perjury exposure for their statements that disputed material is not infringing,[503] along with U.S. federal court jurisdiction and process.[504] According to OSPs interviewed by one of us as part of a qualitative study, the perceived risk to targets of misstating their rights to post contested material chills counternotices.[505] Indeed, it can chill OSPs from encouraging users to submit counternotices, even when they think counternotices are warranted.[506] This is neither a practically usable contestation process, nor one that garners legitimacy.

---

501. Because remedies for copyright liability can be punishing, the DMCA incentivizes online service providers to reduce risk by erring on the side of removing material. Statutory damages range from $200 to $150,000, per work infringed. 17 U.S.C. § 504(c). Because statutory damages are calculated per work infringed, OSPs—which may host or link to very large numbers of user posted works—can face extremely high potential awards. For a detailed discussion of the effect of statutory damages in the U.S. copyright system, see Samuelson & Wheatland, supra note 360. Some have argued that the RTBF also skews too heavily toward takedowns because companies have an incentive to avoid liability for posting personal information in violation of data protection law. See, e.g., Keller, supra note 397, at 320–22. At the same time, companies also appear to have other incentives, both principled and economic, to push back against delisting. For example, Google has developed the practice of placing notices in search results from which links have been delisted and notifying webmasters of removal, despite criticism from regulators. Article 29 Working Party, Guidelines on Google Spain, supra note 308, at 9 subsec. 22, 10 subsec. 23. Indeed, in 2016, the Spanish Data Protection Authority fined Google €150,000 for communicating allegedly identifiable information about three data subjects to webmasters. See David Erdos, Communicating Responsibilities: The Spanish DPA Targets Google's Notification Practices When Delisting Personal Information, Inforrm's Blog (Mar. 21, 2017), https://inforrm.wordpress.com/2017/03/21/communicating-responsibilities-the-spanish-dpa-targets-googles-notification-practices-when-delisting-personal-information-david-erdos/ [https://perma.cc/G5Q3-3XX4].

502. Compare 17 U.S.C. § 512(c)(3)(A)(i-v), with id. § 512(c)(3)(A)(vi).

503. Id. § 512(g)(3)(C).

504. Id. § 512(g)(3)(D).

505. Urban et al., Notice and Takedown in Everyday Practice, supra note 287, at 44–45.

506. Id. at 45. At the same time, these requirements fail to deter bogus counternotices from some bad actors, determined pirates operating from the safety of jurisdictions outside the United States, who are undeterred by perjury penalties or section 512(f) damages. Id. at 46. For example, one rights holder interviewed as part of the *Notice and Takedown in Everyday Practice* research described

> receiv[ing] only seven [counter] notices in the last two years (we have sent nearly 9,000 notices to Google). Two were a result of administrative errors on our end. Five were [bogus counternotices] from Russian or Ukrainian

4. *Regulatory Context and Systemic Regulation.* — Both the substantive rights underlying a contestation scheme and the regulatory design around it can influence how the scheme operates in practice and whether it is perceived as legitimate. For example, the DMCA's section 512 exists against the backdrop of substantive copyright law, including cases on intermediary liability. The RTBF is backstopped both substantively and institutionally by judges (the CJEU) and regulators (data protection authorities enforcing the GDPR). Determining how the regulatory setting affects a right to contest may be particularly challenging for general-purpose algorithmic contestation schemes like Article 22, which are intended to work across legal and market sectors.

Again, an individual right to contest AI is both necessary and by itself insufficient. As noted in section II.B.I, there have been extensive and valid critiques of a regulatory model that relies primarily on individual rights, given the United States' history of emphasizing individual notice and choice.[507] Relying only on individual contestation could in the best case still forgo the benefits of effective systemic regulation of AI, and in the worst case, afford a stamp of legitimacy to an illegitimate system.[508]

Effective governance of AI requires expertise in both substantive law and in technology—expertise that is expensive to acquire, and that most individuals will not have, but that regulators may be more effective at obtaining and applying. Many of the problems with AI, too, are best addressed ex ante—by, for example, inspecting parameters and training sets or involving affected stakeholders—before a system is deployed. And many of the problems with AI will be best assessed systemically, rather than on a case-by-case basis—for example, an AI's impact on particular marginalized groups or physical settings.[509]

Thus it is crucial to situate contestation rights within regulatory oversight and other systemic risk mitigation measures.[510] For example, Slovenia's implementation of the right to contest contains a proactive procedural requirement that a "specially focused impact assessment" be carried out "*[p]rior* to the introduction of a system of automated decision-

---

> torrent sites that knew that there was no chance that we would sue them in their jurisdiction.

Id.

507. See supra notes 242–245 and accompanying text.

508. Edwards & Veale, supra note 175, at 67 (similarly discussing the individual Article 22 "right to explanation" as potentially being a "transparency fallacy").

509. See, e.g., Kaminski, Binary Governance, supra note 12, at 1579 ("An accountable collaborative governance regime can also complement individual procedural rights. Establishing systemic accountability in a collaborative governance regime can bolster individual rights by providing oversight in the name of affected individuals.").

510. See id. at 1549; Margot E. Kaminski, Regulating AI Risk Through the GDPR 13 (unpublished manuscript) (on file with the *Columbia Law Review*).

making procedures."[511] This must "include an impact assessment on related human rights and fundamental freedoms, in particular with regard to nondiscrimination."[512] Other measures, such as requiring that technology be designed ex ante to protect human rights, requiring companies to involve an independent corporate officer in internal decisions and oversight, or requiring external audits of the system, all can make contestation rights more fair and effective. Legislators can backstop these systems with substantive regulations and significant penalties for failure. Individual rights and systemic governance are not in opposition; they can complement and augment each other.[513]

Further, a privatized right to contest cannot be legitimate without some form of systemic transparency. Transparency into how a contestation system is operating and whether it meets due process goals is crucial for accountability and oversight. Subjecting decisions to public transparency over time—a core element of judicial process—can illustrate whether a contestation scheme is systemically accurate or fair. Strikingly, the Council of Europe's Recommendations recommend systemic transparency for contestation.[514]

Yet transparency is often lacking in privatized contestation schemes. For example, the DMCA operates with a considerable lack of transparency and ensuing uncertainty about its reliability.[515] Leaving aside the small number of section 512(f) lawsuits, the DMCA has no transparency requirements. Rather, its contestation scheme operates as a "black box" in which private complainants, websites, and targets make decisions without insight into others' actions.[516] There is no requirement for websites or other parties to disclose their policies, provide their frameworks for decision-making, or explain their decisions.[517] As a result, the U.S. Copyright Office has lamented that

511. Malgieri, Automated Decision-Making in the EU Member States, supra note 115, at 18.

512. Id. With this provision, Slovenia appears to be requiring a specialized version of the "Data Protection Impact Assessments" (DPIAs) required by Article 35 for all processing "likely to result in a high risk to the rights and freedoms of natural persons." GDPR, supra note 13, art. 35(1). Malgieri argues that DPIAs are generally required for algorithmic decision-making but sees the "human rights" aspect of Slovenia's specialized impact assessment as different from the general requirement. Malgieri, Automated Decision-Making in the EU Member States, supra note 115, at 18.

513. Kaminski, Binary Governance, supra note 12, at 1577–80; see also Kaminski & Malgieri, Impact Assessments, supra note 287, at 126–27.

514. Council of Eur., Recommendation on the Human Rights Impacts of Algorithmic Systems, supra note 20, at 13 ("[Companies] should make public information about the number and type of complaints made by affected individuals or groups . . . .").

515. Urban et al., Notice and Takedown in Everyday Practice, supra note 282, at 113, 119–20.

516. See, e.g., Bar-Ziv & Elkin-Koren, supra note 373, at 343–44; Urban et al., Accounts of Everyday Practice, supra note 374, at 374.

517. Although some companies voluntarily provide statistical "transparency reports" and/or contribute notices they receive to the research repository Lumen, this is a minority, and there is no standard for what information is required. This lack of a standard has led to calls for greater voluntary transparency with standardized reporting. See, e.g., Manila

"the privatized, extra-judicial nature of takedown notices and counter-notices under section 512 . . . result[s] in much of the information about how the system is being utilized in practice being inaccessible."[518] The Copyright Office named this as "a key obstacle" for "policy makers looking to create evidence-based policy with respect to the notice-and-takedown regime."[519]

Similarly, RTBF transparency, while encouraged in regulators' Guidelines,[520] is neither mandatory nor consistent. This, too, creates questions about the legitimacy of the system. Google, for example, has set up some transparency processes and described at least some of the substantive criteria it currently uses to render decisions, but the full criteria are unclear.[521]

Systemic transparency could take a number of forms. Record-keeping about decisions and challenges could be made available to the public or to regulators.[522] If this is too onerous, other options could partially fill the gap. For example, the European Commission Guidelines' "good practice suggestions" for algorithmic decisions—auditing, certification, and ethical review boards—could also be applied to contestation mechanisms.[523]

Principles on Intermediary Liability, ManilaPrinciples.Org, https://www.manilaprinciples.org [https://perma.cc/E4DV-N9H8] (last visited Aug. 2, 2021); The Santa Clara Principles on Transparency and Accountability in Content Moderation, SantaClaraPrinciples.Org, https://santaclaraprinciples.org/ [https://perma.cc/T4YD-AHLV] (last visited Aug. 2, 2021).

For examples of "transparency reports," see, e.g., Transparency Report, Google, https://transparencyreport.google.com [https://perma.cc/5HEX-QTVY] (last visited Aug. 2, 2021); Content Removal Requests Report, Microsoft, https://www.microsoft.com/en-us/corporate-responsibility/content-removal-requests-report [https://perma.cc/FU3E-UVVG] (last visited Aug. 2, 2021). Contributors to the Lumen database can be found at Lumen, https://lumendatabase.org [https://perma.cc/2KEN-9TR2] (last visited Aug. 2, 2021).

518. Strong, supra note 310, at 70.

519. Id.

520. Article 29 Working Party, Guidelines on Google Spain, supra note 308, at 3 ("[T]he . . . Working Party . . . strongly encourages the search engines to . . . make more detailed statistics available.").

521. Google voluntarily set up several different sources of transparency regarding the EU's Right to Be Forgotten. For example, it has provided webmasters with notice of removals, Lee, supra note 395, at 1041, and issued a summary report. Theo Bertram, Elie Bursztein, Stephanie Caro, Hubert Chao, Rutledge Chin Feman, Peter Fleischer, Albin Gustafsson, Jess Hemerly, Chris Hibbert, Luca Invernizzi, Lanah Kammourieh Donnelly, Jason Ketover, Jay Laefer, Paul Nicholas, Yuan Niu, Harjinder Obhi, David Price, Andrew Strait, Kurt Thomas & Al Verney, Google, Three Years of the Right to Be Forgotten 2 (2018), https://drive.google.com/file/d/1H4MKNwf5MgeztG7OnJRnl3ym3gIT3HUK [https://perma.cc/3LEC-QDDW]. Google also responded to regulators' encouragement by running an actively updated transparency report that covers the RTBF. See Requests to Delist Content Under European Privacy Law, Google, https://transparencyreport.google.com/eu-privacy/overview?hl=en [https://perma.cc/N94J-ZPD5] (last visited Aug. 2, 2021). Google reports numbers of URLs delisted, categories of requesters, categories of material targeted by removal requests, and statistics including the percentage delisted or retained. Id.

522. See, e.g., the recently proposed Washington Privacy Act, S.B. 5062, 67th Leg., 2021 Reg. Sess. (Wash. 2021) (requiring data protection impact assessments to be made available to the state Attorney General); see also Algorithmic Accountability Act, S. 1108, 116th Cong (2019).

523. Guidelines on Automated Individual Decision-Making, supra note 115, at 32.

C. *A Floor, Not a Ceiling*

AI creates problems wherever it goes. Thus, a right to contest AI decisions with significant effects should attach to the technology and apply across sectors, not just to specific applications. This recommendation runs counter, however, to the current U.S. sectoral approach to regulating information privacy.

Therefore, a right to contest in the United States should operate as a floor, not a ceiling. This approach would allow decisions in particular subject matter areas to receive added protections. This Article has already mentioned criminal law. Perhaps housing, employment, and credit decisions should also receive augmented protections, grounded in existing regulatory regimes.[524] A right to contest could be designed so that in addition to subject-matter-specific laws, regulatory guidance could help fill in sector-specific applications, as could co-regulatory tools such as codes of conduct.[525]

D. *Thresholds for Coverage*

It is beyond the scope of this Article to delineate which kinds of decisions should be subject to a contestation right. However, a right to contest AI should apply at least to decisions with significant effects, even in the private sector. And a right to contest AI should apply not just to decisions made solely by AI, but to human decisions that significantly rely on AI tools.

Due process rights, in general, wax and wane with the importance of the underlying interest. The GDPR's contestation right applies to decisions with "legal" or "similarly significant[]" effects.[526] We leave to policymakers and other research what kinds of decisions have sufficiently "significant effects" to necessitate contestation rights. The Council of

524. See, e.g., Fair Credit Reporting Act, 15 U.S.C. § 1681 (2018); Equal Credit Opportunity Act, 15 U.S.C. § 1691 et seq. (2018).

525. Dennis D. Hirsch, Going Dutch? Collaborative Dutch Privacy Regulation and the Lessons It Holds for U.S. Privacy Law, 2013 Mich. St. L. Rev. 83, 122–35; Dennis D. Hirsch, The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?, 34 Seattle U. L. Rev. 439, 465–66 (2011); Kaminski, Binary Governance, supra note 12, at 1574; William McGeveran, Friending the Privacy Regulators, 58 Ariz. L. Rev. 959, 983–85 (2016).

526. GDPR, supra note 13, Recital 71; see also Guidelines on Automated Individual Decision-Making, supra note 115, at 21–22, which describes "legal effects" as applying to fundamental rights (such as freedom of association and voting), legal status (such as denial of citizenship), recourse to entitlements or benefits, and rights under a contract. "Similarly significant" effects are effects that have an impact on a data subject similar to a change in legal rights in terms of its effects on the data subject's "circumstances, behaviour or choices." The Working Party notes that it "is difficult to be precise about what could be considered sufficiently *significant*," but suggests that access to credit, health services, employment or education might qualify, and that vulnerable individuals might be significantly affected even when others are not. Id.

Europe's Recommendation, for example, contemplates impacts on human rights and democratic systems.[527]

As noted, there is an active policy debate over whether only "solely" algorithmic decisions should be regulated or whether regulations should apply more broadly to cover human decisions facilitated by machines.[528] While the GDPR covers only "solely" automated decisions (although guidance has interpreted this to include at least rubber-stamping humans), the proposal of the Office of the Privacy Commissioner of Canada suggests dropping the qualifier to cover the use of AI more broadly.[529] Proposed legislation in the United States similarly would have applied to AI that helps make impactful decisions.[530] Because regulation could be easily evaded by using a human to rubber-stamp what is essentially an AI process, and because of concerns about human competence to question AI tools, this broader definition is preferable.

E. *Exceptions and Challenges*

While a right to contest AI should in general function as a cross-sectoral floor, it may make sense to carve out exceptions for some applications or to tailor the threshold for coverage so that some applications aren't included. In some cases, it may be that some other oversight mechanism—for example, expert oversight by a doctor with a fiduciary duty to a patient[531]—adequately substitutes for an individual right to contest. In others, it may be that the right's threshold coverage could be tailored to leave out some kinds of arguably significant effects, such as telecommunications network outages.[532] Future research may address this question.

---

527. See Council of Eur., Recommendation on the Human Rights Impacts of Algorithmic Systems, supra note 20, at 6, 9, 11, 13.

528. See supra notes 115, 150, 307 and accompanying text.

529. See GDPR, supra note 13, art. 22(1); Guidelines on Automated Individual Decision-Making, supra note 115, at 7 (explaining that an activity may still be "solely" automated processing even if there is human involvement). The Office of the Privacy Commissioner of Canada states:

> PIPEDA will need to define automated decision-making to create specific protections to apply to it. Unlike the GDPR or Quebec's Bill 64, the term should drop any qualifier such as "solely" or "exclusively", which scopes the applicability of specific protections very narrowly. These also make the term susceptible to subversion where a human role is added in the process to merely evade additional obligations.

Off. of the Priv. Comm'r of Can., supra note 23.

530. Algorithmic Accountability Act, S. 1108, 116th Cong. § 2(1) (2019) (defining an automated decision system as "a computational process, including one derived from machine learning, statistics, or other data processing or artificial intelligence techniques[] that makes a decision or facilitates human decision making[] that impacts consumers").

531. Kluttz et al., supra note 27, at 22–23.

532. See USM Sys., How Artificial Intelligence Is Used in the Telecom Industry?, Medium (Aug. 17, 2020), https://usmsystems.medium.com/how-artificial-intelligence-is-used-in-the-telecom-industry-dd65459a220a (on file with the *Columbia Law Review*) (explaining that AI can support monitoring equipment to prevent outages and network disruptions).

Significant open questions and challenges remain. For example, under what circumstances, if any, should policymakers allow for unexplainable AI? Relatedly, what level of explainability is necessary for effective contestation? The EU suggests that a right to explanation and right to contestation are intertwined, but that might not always be the case. Centralizing the right to contest—versus the right to meaningful explanation—might address some of the purportedly irreconcilable challenges of black-box AI, if an effective contestation scheme could be designed without necessarily opening the black box. One way to do so might be to give individuals performance metrics and allow contestation on the basis of disparate impact on a particular group.[533]

Other questions, however, remain. What happens if there is a clear tradeoff between affording a right to contest and accuracy? Or between affording a right to contest and bias across a system? Again, these are problems for future researchers, but a look to the due process literature might be informative.

CONCLUSION

Returning now to the International Baccalaureate students whose story begins this Article, the importance of the right of contestation becomes clear. Writing in the *Harvard Business Review*, a parent of an IB student and two colleagues argue that the IBO should have designed a more contestable process.[534] "[Better design] is about making sure that people understand what information is used in assessing grades and what the steps are in the appeals process itself."[535] This argument invokes both dignity (participation) and rule of law (transparency) values. In other words, people confronted with AI decision-making look for more transparency, more explanation, and more participation: a right to contest.

There is a growing momentum around the world for establishing a right to contest AI decisions. This right has an important role to play in the United States, where it is not yet a meaningful part of policy conversations. A right to contest AI is both normatively desirable and practically feasible. A right to contest could ameliorate the foreseeable harms of AI.

533. See Edwards & Veale, supra note 175, at 55–56 (explaining that performance metrics give information on a model's unseen data, including breakdowns like success in certain subcategories of data).

534. Evgeniou et al., supra note 45 (arguing that IBO should have created an easier appeals process that offered human-led re-evaluation of grades).

535. Id.