Yale Journal of Law & Technology
Volume 27, Issue 1

Impacted Stakeholder Participation in AI and Data Governance

Margot E. Kaminski* **& Gianclaudio Malgieri****

Privacy law has long centered on the individual. But we observe a meaningful shift toward group harm and rights. There is growing recognition that data-driven practices, including the development and use of artificial intelligence (AI) systems, affect not just atomized individuals but also their neighborhoods and communities, including and especially situationally vulnerable and historically marginalized groups.

This Article explores a recent shift in both data privacy law and the newly developing law of AI: a turn towards stakeholder participation in the governance of AI and data systems, specifically by impacted groups often though not always representing historically marginalized communities. In this Article we chart this development across an array of recent laws in both the United States and the European Union. We explain reasons for the turn, both theoretical and practical. We then offer analysis of the legal scaffolding of impacted stakeholder participation, establishing a catalog of both existing and possible interventions. We close with a call for reframing impacted stakeholders as rights-holders, and for recognizing several variations on a group right to contest AI systems, among other collective means of leveraging and invoking rights individuals have already been afforded.

---

* Professor of Law, Colorado Law School; Director, Privacy Initiative, Silicon Flatirons Center; 2024 Fulbright-Schuman Grantee; 2024 Fernand Braudel Senior Fellow at the European University Institute (EUI); 2023-2025 Faculty Associate at the Harvard Berkman Klein Center; Affiliated Fellow, Information Society Project at Yale Law School. Many thanks to, among others, Federica Casarosa; Mariavittoria Catanzariti; Mateus Correia De Carvalho; Ngozi Okidegbe; Jen Raso; Ariana Rossi; Albert Sanchez-Graells; faculty at the University of Bristol Law School; participants in the paper workshop at the EUI; the participants at the eLaw Leiden workshop in March 2024; and participants at Privacy Law Scholars Conference 2023.

** Associate Professor of Law, Leiden University (eLaw Center for Law and Digital Technologies); Co-Director, Brussels Privacy Hub. Many thanks to, among others, Simone van der Hof, Bart Custers, Francien Dechesne, Carlotta Rigotti, and all the participants at the eLaw Leiden workshop in March 2024.

Article Contents

Introduction

Privacy law has long centered on the individual: the person whose home life was captured by surreptitious photographers,[1] the lovers whose image was published without their permission,[2] and the labor organizer whose phone call was tapped.[3] Privacy laws, including data privacy laws, have thus historically afforded a set of rights to individuals.[4] Recently enacted U.S. laws, for example, afford individuals a right to say no to the sale of one's data and a right to opt out of some types of data profiling.[5] But something else is afoot.

There is growing recognition that data-driven practices, including the development and use of Artificial Intelligence (AI) systems, impact not just atomized individuals but neighborhoods, communities, and groups. For example, the Fourth Circuit evaluated the city of Baltimore, Maryland's aerial surveillance of majority Black neighborhoods for its impact not just on individuals but on entire historically marginalized communities.[6] The court noted that "mass surveillance 'touches everyone, but its hand is heaviest in communities already disadvantaged by their poverty, race, religion,

---

[1] Samuel D. Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 206 (1890); William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 389 (1960).
[2] Gill v. Hearst Pub. Co., 253 P.2d 441, 442 (1953); RESTATEMENT (SECOND) OF TORTS § 652D cmt. b, illus. 6 (AM. L. INST. 1977).
[3] Bartnicki v. Vopper, 532 U.S. 514, 517–18 (2001).
[4] Woodrow Hartzog, *The Inadequate, Invaluable Fair Information Practices*, 76 MD. L. REV. 952, 952–53 (2017).
[5] CAL. CIV. CODE §§ 1798.100–1798.199 (West 2018); Cal. Privacy Rights Act (2020) (amending same); COLO. REV. STAT. ANN. § 6-1-1301 (2022).
[6] *Leaders of a Beautiful Struggle v. Baltimore Police Department*, 2 F.4th 330, 348 (4th Cir. 2021) ("[L]iberty from governmental intrusion can be taken for granted in some neighborhoods, while others 'experience the Fourth Amendment as a system of surveillance, social control, and violence, not as a constitutional boundary that protects them from unreasonable searches and seizures.'" (quoting Devon W. Carbado, *From Stopping Black People to Killing Black People: The Fourth Amendment Pathways to Police Violence*, 105 CALIF. L. REV. 125, 130 (2017)). *See also Recent Cases: Fourth Circuit Holds Warrantless Access of Aerial Surveillance Data Unconstitutional*, 135 HARV. L. REV. 920, 924 ("The Fourth Circuit judges clearly embraced these dynamics in their extensive discussions of racial equity and policing issues, echoing many of the lessons of the ongoing Black Lives Matter social movement.").

ethnicity, and immigration status.'"[7]

Information affords power, and power lends itself to social control. There has long been a link between surveillance and racism. As former Federal Trade Commission (FTC) Commissioner Alvaro Bedoya observes, the U.S. government regularly surveilled leading civil rights era leaders, including Martin Luther King Jr., for purposes of social control.[8] Bedoya writes: "[W]hen we talk about privacy only as a civil liberty, we erase those patterns of harm, that color of surveillance . . . . Surveillance threatens vulnerable people fighting for equality. Privacy is what protects them and makes it possible."[9]

The harms of AI systems, too, are increasingly understood to be not just individual but also communal and relational. Discriminatory hiring algorithms can be biased against women, [10] or disproportionately turn down job applicants with legally protected disabilities.[11] One person's decision to share their data can lead to the creation of inferences then used in the profiling and data-driven manipulation of many others.[12] Sharing one's DNA with a private company implicates not just your own privacy but the privacy and freedom of your family members.[13]

This Article explores a nascent and important shift in both data privacy law and the newly developing law of AI: a turn to stakeholder participation, specifically by impacted groups, often

---

[7] *Leaders of a Beautiful Struggle*, 2 F.4th at 347 (quoting BARTON GELLMAN & SAM ADLER-BELL, CENTURY FOUND., THE DISPARATE IMPACT OF SURVEILLANCE 2 (2017) (cleaned up)).

[8] Alvaro M. Bedoya, *Privacy as Civil Right*, 50 N.M. L. REV. 301, 311 (2020).

[9] *Id.* at 306.

[10] Samantha Cole, *Amazon Pulled the Plug on an AI Recruitment Tool That Was Biased Against Women*, VICE (Oct. 10, 2018, 11:49 AM), https://www.vice.com/en/article/evwkk4/amazon-ai-recruitment-hiring-tool-gender-bias [https://perma.cc/B4Z7-QHP5].

[11] U.S. EQUAL EMP. OPPORTUNITY COMM'N, *The Americans with Disabilities Act and the Use of Software, Algorithms, and Artificial Intelligence To Assess Job Applicants and Employees*, EEOC-NVTA-2022-2 (May 12, 2022), https://www.eeoc.gov/laws/guidance/americans-disabilities-act-and-use-software-algorithms-and-artificial-intelligence [https://perma.cc/2ASA-9RTS].

[12] Salomé Viljoen, *A Relational Theory of Data Governance*, 131 YALE L.J. 573, 578 (2021); Alicia Solow-Niederman, *Information Privacy and the Inference Economy*, 117 NW. U. L. REV. 357, 361 (2022).

[13] Jasmine McNealy, *An Ecological Approach to Data Governance*, 37 NOTRE DAME J. OF L., ETHICS & PUB. POL. ONLINE SUPP. 523, 525–27 (2023).

though not always representing historically marginalized communities. This turn to impacted stakeholder participation is more complex and varied than it might first appear. It is driven by a growing understanding that privacy harms and AI harms are often collective and often discriminatory, and that data-driven technologies pose particular threats to democratic intervention in their opacity.

A number of both proposed and enacted laws now establish specific avenues for impacted stakeholder participation in governing data processing and AI. For example, the EU's General Data Protection Regulation (GDPR) requires impacted stakeholders to be consulted as part of its impact assessment process.[14] Colorado's facial recognition law created an AI Impact Task Force, which was required to include impacted stakeholders as representatives.[15] Similar stakeholder consultation activities about facial recognition were organized in Canada.[16] The November 2024 draft of California regulations on AI pushed businesses to include impacted stakeholders or their representatives in governance.[17]

In contrast to general calls for public participation, these laws

---

[14] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1 [hereinafter GDPR], art. 35; Article 29 Data Prot. Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679, WP248 rev.01, at 8 (Apr. 4, 2017) [hereinafter Article 29 Data Prot. Working Party, *DPIA*].

[15] COLO. REV. STAT. § 2-3-1707 (2022).

[16] *See* MAURICE JONES AND FENWICK MCKELVEY, NORTHERN LIGHTS AND SILICON DREAMS: AI GOVERNANCE IN CANADA (2011-2022) 55-72 (Fenwick McKelvey, Sophie Toupin, and Jonathan Roberge, eds. 2024).

[17] California Privacy Protection Agency, Proposed Text of Regulations (CCPA Updates, Cyber Risk, ADMT, and Insurance Regulations), § 7151(b) (proposed Nov 22, 2024) [hereinafter Proposed CPPA Regulations], https://cppa.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_ins_text.pdf [https://perma.cc/GX4A-FV3J] ("A risk assessment may involve external parties to identify, assess, and mitigate the risks to consumers' privacy. These external parties may include, for example, service providers, contractors, experts in detecting and mitigating bias in automated decisionmaking technology, a subset of the consumers whose personal information the business seeks to process, or stakeholders that represent consumers' or others' interests, including consumer advocacy organizations.")

and guidance create *specific and tailored mechanisms* for *impacted groups and communities*—often, though not always, historically marginalized communities—to have a say about data processing and AI systems that affect them. In this Article we chart this development across an array of laws in Part I.

We then explain in Part II *why* the turn to stakeholder participation has developed: what we believe are its varied origins, both theoretical and as a matter of political economy. On the one hand, there are a number of theoretical explanations for this turn to impacted stakeholder participation. It reflects both criticisms of AI and related technologies as inherently undemocratic and calls for recognition of the collective nature of privacy and AI harms.[18] And it reflects acknowledgments of the particularly destructive nature of those harms to historically marginalized people and communities. These harms have been well-documented, from the use of racist recidivism risk assessments to biased decisions by hiring algorithms to what Anita Allen has termed "discriminatory oversurveillance."[19] The turn to impacted stakeholder participation also reflects calls for "bottom-up" governance by communities most impacted by data processing and AI.[20] It reflects "design thinking:" the development of "participatory design" and related methodologies, which emphasize building technologies for the people who use and will be impacted by them.[21]

But the turn to stakeholder participation also reflects political forces and recent legal history. Through this lens, the origins of impacted stakeholder participation in AI law and data privacy law are complex. They echo a turn to community participation in governance of policing and policing technologies, in the United

---

[18] *See e.g.*, Viljoen, *supra* note 12, at 578; Solow-Niederman, *supra* note 12, at 361.

[19] Anita L. Allen, *Dismantling the "Black Opticon": Privacy, Race, Equity, and Online Data-Protection Reform*, 131 YALE L. J. FORUM. 907, 911 (2022).

[20] Ngozi Okidegbe, *To Democratize Algorithms*, 69 UCLA L. REV. 1688, 1729–31 (2023); Hannah Bloch-Wehba, *Algorithmic Governance from the Bottom Up*, 48 BYU L. REV. 69, 89–90 (2022).

[21] Meg Young, Lassana Magassa & Batya Friedman, *Toward Inclusive Tech Policy Design: A Method for Underrepresented Voices to Strengthen Tech Policy Documents*, 21 ETHICS & INFO. TECH. 89, 92–93 (2019) (discussing a method for vetting tech policy as artifacts through value-sensitive design method called Diverse Voices; SASHA COSTANZA-CHOCK, DESIGN JUSTICE: COMMUNITY-LED PRACTICES TO BUILD THE WORLDS WE NEED 85–88 (2020).

States in particular, reflecting calls for racial justice.[22] They also, however, reflect an increasing reliance on risk regulation—a particular managerial form of governance that stems from data protection law in the EU and enterprise risk management in the United States—in which regulators use vague terms and take more of a back seat to in situ organizational governance.[23]

The convergence of *community governance* on the one hand and *risk management* on the other is shaping impacted stakeholder participation in practice. That is, the push for bottom-up governance and design justice is converging with neoliberal regulatory trends towards co-governance and enterprise risk management. Both trends now prioritize stakeholder participation, but often towards very different goals. This odd alliance has been shaping and stretching the practical mechanisms of at least some forms of stakeholder participation: as softer interventions rather than mandates, as vague nods rather than requirements with pragmatic procedural details, and as a way to *manage risks* rather than *opt out* of extractive data practices and the use of AI systems—despite what many calling for impacted stakeholder participation might wish.[24]

Reflecting these diverse reasons and forces, the legal mechanisms of stakeholder participation are not uniform. By surveying a wide array of practices and policy proposals regarding impacted stakeholder participation, this Article in Part III establishes a catalog of possible interventions. This catalog reflects existing and proposed laws and goes beyond them. It examines, among other things, attempts to define impacted stakeholders, the timing of stakeholder interventions, and capacity-building, including access to information and expertise.

We argue that to craft effective stakeholder participation, one

---

[22] *See, e.g.*, Amna A, Akbar, *An Abolitionist Horizon for (Police) Reform*, 108 CALIF. L. REV. 1781, 1834–37 (2020); Julian Clark & Barry Friedman, *Community Advisory Boards: What Works and What Doesn't (Lessons from a National Study)*, 47 AM. J. CRIM. L. 159, 161–62 (2020) [hereinafter CAB Study]; Okidegbe, *supra* note 20, at 1729–31.

[23] Margot E. Kaminski, *Regulating the Risks of AI*, 103 B.U. L. REV. 1347, 1402–03 (2023).

[24] Margot E. Kaminski, *The Developing Law of AI: A Turn to Risk Regulation*, LAWFARE 2 (Apr. 21, 2023), https://www.lawfaremedia.org/article/the-developing-law-of-ai-regulation-a-turn-to-risk-regulation [https://perma.cc/XQH3-ATPY]; Okidegbe, *supra* note 20, at 1734–37 (calling for veto power in community governance of carceral algorithms).

must understand why one is establishing stakeholder participation in the first place.[25] This will be a particularly challenging task given the divergence in reasons and motivations among proponents of the stakeholder model. Aware that we cannot solve all problems of democratic participation or participatory design here (and indeed, researchers in other disciplines may be better situated to address those questions), we aim instead to prompt critical thinking about the *legal scaffolding for impacted stakeholder participation* in the law of data privacy and AI. We examine how the law might be made better and the likely limits and sources of pushback, given how the turn to stakeholder participation has emerged.

That is, we write not about how to solve the problem of stakeholder participation in general but about how to better write or implement laws on privacy, data governance and AI. We call for understanding and crafting impacted stakeholder rights not in isolation but with a systemic understanding of how these rights interrelate to other forms of accountability. Stakeholder participation in data governance and AI governance should be understood as a necessary but not sufficient aspect of what we here call *robust accountability*. Different forms of accountability interact with each other in both data privacy law and AI law, and stakeholder participation cannot and does not stand alone.

We close with a call for reframing impacted stakeholders as *rights-holders* and recognizing several variations on a group right to contest AI—to challenge the output of such systems once they are in place and to have such challenges make a meaningful difference as to system design or even ongoing system use. Impacted rights-holders should not just be consulted about the design of systems as-applied or involved with policymaking at a high level. They should be empowered to collectively leverage and invoke the kinds of rights they as individuals are already afforded, including through both existing groups and new organizations.

---

[25] Margot E. Kaminski, *Understanding Transparency in Algorithmic Accountability*, *in* THE CAMBRIDGE HANDBOOK OF THE LAW OF ALGORITHMS 121, 121 (Woodrow Barfield ed., 2020) ("[D]etermining the who, what, when, and how of transparency requires first addressing the question of why.").

I. The New Law of Impacted Stakeholder Participation in Data Privacy and AI Governance

Accountability—to both affected individuals and regulators—has long been a critical aspect of data privacy law. This is because, at its core, data privacy is about power more than it is about control. Data privacy is centrally concerned with redressing power imbalances when personal information is housed not with individuals but with large and largely unresponsive entities, whether governmental or private.

"Algorithmic accountability," the recent precursor to AI law, is also largely concerned with establishing accountability over often "black-box" systems. The developing law of AI–provisions in data protection laws—including the EU AI Act, the EU's Digital Services Act, the National Institute of Standards and Technology (NIST) AI Risk Management Framework, and state laws—focuses to a large degree on accountability as a core value in response to what are understood to be particularly opaque systems.

Recent accountability efforts are notable in that they tend to structure accountability to impacted stakeholders as groups. Data privacy law has long focused on the individual and empowered regulators to stand in for societal interests. But it has left a gap in the middle when it comes to group and relational harms.[26] This is now changing in both the literature and the law.

We observe an emerging trend: *A number of newer data protection and AI laws attempt to directly involve stakeholders impacted by the use of surveillance or AI technologies, or their representatives, as a way of addressing group or communal concerns.* These newer data protection and algorithmic accountability laws specifically propose new processes for seeking out members of impacted communities for their input in policymaking and enforcement. Sometimes these laws specifically reference impacted marginalized groups; sometimes the requirements do not mention historic marginalization or situational vulnerability, just the fact of impact. But this overarching trend towards impacted stakeholder participation has been emerging in both the European Union and the United States.

In this Part, we offer examples of this turn. Impacted stakeholder participation is contemplated in an array of recent laws, both enacted

[26] Viljoen, *supra* note 12 at 578; Solow-Niederman, *supra* note 12 at 360–62.

and proposed, and in both hard law and softer guidance. It exists relatively unnoticed alongside other recent attempts to establish accountability to third parties, including experts and auditors.

We start with community governance of surveillance technologies used in policing in the United States. Next, we turn to the EU's GDPR as a leading example of stakeholder participation in data protection. We then discuss the EU AI Act. Finally, we highlight several recent U.S. examples, including in the closest thing to a federal omnibus AI Law, the guidance on AI Risk Management from NIST. The set of laws that we choose to discuss is selective, not exhaustive; we refer to additional laws in Part III when establishing a catalog of stakeholder participation and how to improve it. The purpose of this Part is to convince the reader: the turn to impacted stakeholder participation is happening, and it's a growing trend.

A. Community Advisory Boards

Community advisory boards in the United States represent an attempt to involve impacted stakeholders or their representatives in the governance of policing. Some of these boards have governed police adoption of technologies such as body cameras, cell-site simulators, crime mapping and crime forecasting, and other community-wide surveillance systems.[27] Legal experts who focus on omnibus data privacy laws may overlook the role of community advisory boards as data governance. These boards don't look like other data privacy laws. But any discussion of impacted stakeholder participation in data privacy or AI law would be weakened by failing to address them as an early example.

Community advisory boards represent an attempt at "front end" or ex-ante community governance of policing, in contrast to after-the-fact investigations of officer misconduct.[28] Versions of these boards have been around since as early as the 1960s, but they more recently proliferated across the United States in the 2010s in response to tragic accounts of police violence against Black people and oversurveillance of Black and Brown communities.[29] As the

---

[27] *See*, *e.g.*, CAB Study, *supra* note 22, at 167 (on board oversight over body camera policy in Richland County, South Carolina).

[28] *Id.* at 6; Barry Friedman & Maria Ponomarenko, *Democratic Policing*, 70 N.Y.U. L. REV. 1827, 1877 (2015).

[29] CAB Study, *supra* note 22, at 3.

name indicates, community advisory boards assemble community members to offer advice to the police on an array of topics, including surveillance technologies.[30] Some boards are created informally, while others are established by city ordinance.[31] Their output is typically advisory rather than binding in nature.[32]

The Oakland Privacy Advisory Commission (OPAC) offers a particularly salient example of a community advisory board that provides input into decisions specifically around data privacy and the use of surveillance and other technologies.[33] The OPAC was created as one of the first participatory advisory commissions in response to protests and community organization against the city of Oakland, California's plan to create and deploy a mass surveillance system, including cameras in schools and public housing.[34] The OPAC arose as the result of bottom-up protests, not top-down governance.[35]

While the OPAC's by-laws encourage the mayor to select commissioners based on categories that emphasize legal or technical expertise,[36] they also emphasize local community representation,

---

[30] *Id.* at 5-7 (describing board oversight over body camera policy in Richland County, South Carolina).

[31] *Id*. at 6.

[32] *Id*.

[33] *Id.* at 12; Okidegbe, *supra* note 20, at 1733-34.

[34] Okidegbe, *supra* note 20 at 1733. *See also* Brian Hofer, *How the Fight to Stop Oakland's Domain Awareness Center Laid the Groundwork for the Oakland Privacy Commission*, ACLU NOR. CAL. (Sept. 21, 2016), https://www.aclunc.org/blog/how-fight-stop-oaklands-domain-awareness-center-laid-groundwork-oakland-privacy-commission [https://perma.cc/CX5K-5EZD]; Cyrus Farivar, *Why Privacy Needs All of Us*, S.F. PUB. PRESS (Dec. 17, 2018), https://www.sfpublicpress.org/why-privacy-needs-all-of-us/ [https://perma.cc/YUD2-R8M4] (describing the makeup of the OPAC in 2018).

[35] Okidegbe, *supra* note 20, at 1733; *see also* Bloch-Wehba, *supra* note 20 (calling for bottom-up algorithmic governance).

[36] Oakland Privacy Commission, Bylaws art. II, § 2(h) ("Members of the Privacy Commission shall represent the following criteria, with no more than two (2) members representing any one criteria and at least one from each criteria to the extent possible: (1) an attorney, legal scholar, or activist with expertise in privacy, civil rights, or a representative of an organization with expertise in the same; (2) a past or present member of member of law enforcement who has worked with surveillance equipment and other technology that collects or stores citizen data; (3) an auditor or certified public accountant; (4) a hardware, software, or

requiring at least six of the nine members to be Oakland residents.[37] OPAC members are currently listed by the district they represent.[38] The OPAC has addressed police use of cell-site simulators (which track location, among other things), facial recognition (used to identify people in crowds and public areas), and automated license plate readers (which scan license plates looking for flagged cars).[39] Each of these surveillance technologies raises concerns about wide scale deployment affecting entire neighborhoods and communities.

Another recent example, even before the OPAC, comes from Seattle, Washington.[40] Any city department that intends to acquire "surveillance technology" must obtain City Council approval before that acquisition.[41] Ordinance 125376 in 2018 established a "Community Surveillance Working Group" to advise the Seattle City Council and the Mayor on police use of surveillance technology "from a community perspective."[42] The Working Group provides a privacy and civil liberties impact assessment in response to each department request for surveillance technology. It additionally provides recommendations to the city's Chief Technology Officer for their required annual equity impact assessment. Among the Working Group's goals is "ensuring members of vulnerable communities have the opportunity to provide input and feedback on

---

encryption security professional; (5) a member of an organization which focuses on government transparency and openness." (cleaned up)), https://cao-94612.s3.us-west-2.amazonaws.com/documents/Bylaws-for-the-Privacy-Advisory-Commission.pdf [https://perma.cc/RY7D-69YW].

[37] *Id.* § 2(a).

[38] *See*, *e.g.*, Privacy Advisory Comm., *Meeting Agenda*, CITY OF OAKLAND, CAL. (Jan. 4, 2024), https://cao-94612.s3.us-west-2.amazonaws.com/documents/Agenda-Packet-for-the-Privacy-Advisory-Commission-Meeting-on-1-4-2024.pdf [https://perma.cc/K7S7-K325].

[39] David DeBolt, *Lauded as a National Model, Some Question Whether Oakland's Privacy Commission is Working*, OAKLANDSIDE (Nov. 2, 2021, 1:28 PM), https://oaklandside.org/2021/11/02/lauded-as-a-national-model-some-question-whether-oaklands-privacy-commission-is-working/ [https://perma.cc/C2TN-K27G].

[40] SEATTLE, WASH., MUN. CODE ch. 14.18, https://library.municode.com/wa/seattle/codes/municipal_code?nodeId=TIT14HURI_CH14.18ACUSSUTE. Many thanks to Ngozi Okidegbe for pointing us to this example.

[41] *Id.* at § 14.18.020(A).

[42] *Id*.

surveillance technology through the… . . . approval process."[43]

The Seattle Working Group consists of seven members, some appointed by the Mayor and some by the City Council. The law dictates that at least five members "shall represent equity-focused organizations serving or protecting the rights of communities and groups historically subject to disproportionate surveillance, including Seattle's diverse communities of color, immigrant communities, religious minorities, and groups concerned with privacy and protest."[44] Notably, the impact assessments that the Group must provide are required to contain "a description of the potential impact of the surveillance technology on civil rights and liberties and potential disparate impacts on communities of color and other marginalized communities."[45]

Discussions of community advisory boards foreshadow many of the policy debates that permeate recent attempts at establishing impacted stakeholder participation in data privacy and AI laws.[46] The boards raise questions about representation, including both who should select representatives,[47] and how representation should be defined.[48] For example, Phoenix constitutes its Advisory Boards by choosing representatives from twelve different local demographic groups, while San Francisco constitutes its boards by choosing representatives by location.[49] There are concerns that those who select Board representatives may mistakenly assume that particular individuals of a particular race, gender, or socioeconomic group represent a broader community.[50]

Community advisory boards also raise issues about capacity building, including providing technical expertise to enable effective

---

[43] *Id.* at § 14.18.080(B)(1-3).
[44] *Id*. at § 14.18.080(A)(3).
[45] *Id*. at 14.18.080(B)(1).
[46] Ngozi Okidegbe suggests looking at the OPAC "as a useful jumping-off point for thinking about how to design an institutional structure with power-building potential." Okidegbe, *supra* note 20.
[47] CAB Study, *supra* note 22, at 6; Okidegbe, *supra* note 20 at 1737-1739 (proposing a selection process analogous to jury selection).
[48] *Id*. 6, 14-15 (offering examples of the San Francisco Police Department's Advisory Boards, which represent citizens by location, with one for each of the city's ten district stations, versus Phoenix, Arizona's board, which has twelve Advisory Boards each of which represents a different demographic group).
[49] *Id*.
[50] *Id.* at 14.

input and providing financial resources to enable board engagement with the community at large.[51] The design of the boards raises, as Ngozi Okidegbe notes, important questions about how to design governance to blend "communal, technocratic, and technological expertise."[52]

Most significantly, the advisory and generally under-resourced nature of these boards raises questions of their efficacy in practice versus their status as performative participation.[53]

B. EU Examples: The GDPR and EU AI Act

If community advisory boards represent local attempts in the United States to govern police surveillance and police use of algorithms arising in response to bottom-up governance, EU data protection laws fold attempts at bottom-up participation into what is a mostly top-down governance regime. In many recent and emerging data protection laws–including the EU's GDPR–there is a new sheriff in town: the third party.[54] Compared to previous data protection laws (e.g., the EU Data Protection Directive), these newer laws explicitly structure participation by both designated third-party experts (such as auditors) and impacted stakeholders or their representatives. Where once such actors were treated either as impacted individuals or as members of the general public, emerging data protection and algorithmic accountability laws loop them into the accountability scheme much more directly. Note that the impacted stakeholders envisioned in Europe's data protection and AI laws are not necessarily historically marginalized or particularly vulnerable stakeholders, at least on the face of the law. They're just stakeholders who are affected by use of the technology.

Europe's massive omnibus data protection regulation, the

---

[51] *Id*. at 10, 13.

[52] Okidegbe, *supra* note 20, at 1739.

[53] CAB Study, *supra* note 22, at 168 ("In many cases, we came to question the utility of CABs"), 168-69 (offering other forms of community engagement, including community meetings and listening sessions).

[54] Margot E. Kaminski, *Binary Governance: Lessons from the GDPR's Approach to Algorithmic Accountability*, 92 S. CALIF. L. REV. 1529, 1536 (2019) ("[W]e need not just transparency and oversight over the algorithm, but second-order transparency and oversight over that rulemaking and compliance process"); IAN AYRES & JOHN BRAITHWAITE, RESPONSIVE REGULATION 57–60 (1992); Ian Ayres & John Braithwaite, *Tripartism: Regulatory Capture and Empowerment*, 16 L. & SOC. INQ. 435, 491 n.137 (1991)

GDPR, which went into effect in 2018, contemplates impacted stakeholder participation in at least two places: the Data Protection Impact Assessment (DPIA) process and regulation of automated decision-making with significant effects.

Under the GDPR, data controllers have an obligation to conduct impact assessments for certain high-risk types of data processing. During the DPIA process, the data controller has a duty to "seek the views of data subjects or their representatives on the intended processing."[55] On paper, this is a significant requirement; however, GDPR guidelines suggest simple surveys could suffice. [56] Additionally, not every data processor is required to conduct an impact assessment, and not every impact assessment is subject to regulatory oversight.

Article 22 of the GDPR includes a more implicit reference to stakeholder participation: the right to not be subject to automated decision-making. [57] This law establishes that, in most cases, companies and government entities cannot use an automated system to make a decision about an individual with significant effects.[58] But it also contemplates allowing automated decision-making in some contexts, subject to "suitable safeguards," some of which are listed in the text.[59] Suitable measures to safeguard rights under the GDPR guidelines include a number of third-party accountability measures,

---

[55] GDPR, *supra* note 14, art. 35(9).

[56] *See* Article 29 Data Prot. Working Party, *DPIA*, *supra* note 14, at 13 (suggesting very limited ways to implement the duty to seek the views of data subjects in Article 35(9), e.g., internal studies and surveys). *But see* Margot E. Kaminski and Gianclaudio Malgieri, *Algorithmic Impact Assessments Under the GDPR: Producing Multi-Layered Explanations*, 11 INTERNATIONAL DATA PRIVACY LAW 125 (2021) (offering critiques of these guidelines).

[57] Kaminski, *supra* note 54 at 1594.

[58] Article 22 of the GDPR refers to "legal or similarly significant effects". Recital 71 mentions, as an example of these effects, "automatic refusal of an online credit application or e-recruiting practices without any human intervention". See more in Gianclaudio Malgieri & Giovanni Comandé, Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation, *International Data Privacy Law*, Volume 7, Issue 4, November 2017, Pages 243–265.

[59] GDPR, *supra* note 14, art. 22(3) (stating that "the data controller shall implement *suitable measures to safeguard* the data subject's rights and freedoms and legitimate interests, 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.") (emphasis added).

including algorithmic auditing, independent third-party auditing, and ethical review boards.[60] It is not a stretch to suggest that data controllers could probably use impacted stakeholder accountability as one such third-party safeguard—especially as data controllers conducting automated decision-making are required to conduct impact assessments, which, as we note above, establish a duty to seek the views of impacted stakeholders in that process.[61]

The European Union AI Act, approved in June 2024, also envisions impacted stakeholder participation in the governance of AI systems. Although early commentators question whether the AI Act is really "participatory," there are evident steps in that direction.[62]

Under the AI Act, certain deployers of AI systems that are classified as "high risk" (e.g., AI systems used for credit scoring; assessment of workers or students; or border control; or used by judges, public administration, and police, among others) are obliged to carry out a "fundamental rights impact assessment" prior to putting their AI systems into use.[63] The impact assessment requires among other things a description of the following: the purposes and the scopes of the AI system, the categories of people affected, the reasonably foreseeable impacts on fundamental rights, and the

---

[60] Article 29 Data Prot. Working Party, Guidelines on Automated Individual Decision-making and Profiling for the Purposes of Regulation 2016/679 (wp251rev.01), 2018, 32.

[61] *See* Article 29 Data Prot. Working Party, Guidelines on Automated Decision-making, 32 referring to "ways to allow the data subject to express his or her point of view and contest the decision" and Article 29 Data Prot. Working Party, *DPIA*, *supra* note 14, at 13 (suggesting ways to implement the duty to seek the views of data subjects in Article 35(9), e.g., internal studies and surveys). *See generally* Margot E. Kaminski and Gianclaudio Malgieri, *Algorithmic Impact Assessments Under the GDPR: Producing Multi-Layered Explanations*, 11 INT'L DATA PRIVACY L. 125 (2021).

[62] *See*, *e.g.*, Johann Laux, Sandra Wachter, & Brent Mittelstadt, *Trustworthy Artificial Intelligence and the European Union AI Act: On the Conflation of Trustworthiness and Acceptability of Risk*, 18 REGUL. & GOVERNANCE 3, 3, 7, 18 (2023).

[63] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence and Amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828, 2024 O.J. (L 1689) 1 [hereinafter EU AI Act], art. 27.

"specific risks of harm likely to impact the categories of persons or group of persons" who are "likely to be affected by its use in the specific context."[64]. Within this framework, the deployers of high-risk AI systems, particularly in the public sector, could (but are not required to) "involve relevant stakeholders, including the *representatives of groups of persons likely to be affected by the AI system*, independent experts, and civil society organizations in conducting such impact assessments and designing measures to be taken in the case of materialization of the risks."[65]

Moreover, the AI Act potentially enables impacted stakeholder participation not only at the level of designing a specific AI system but also at the enforcement level. Following recommendations from civil society,[66] the final text of the AI Act mandates the creation of an Advisory Forum that will provide the AI Office (the new Board that will monitor, coordinate, and ensure consistent application and enforcement of the AI Act) with stakeholder input on application of the Act. The Advisory Forum will be composed of "a balanced selection of stakeholders, including . . . civil society and academia," and its composition shall be "balanced with regard to commercial and non-commercial interests."[67] While the list of participants does not explicitly name impacted stakeholders, it is possible or even likely that civil society organizations will be selected to take those views into account.[68] On the other hand, the AI Act potentially overemphasizes policy expertise over lived experience in that it dictates that the "Commission shall appoint the members of the advisory forum . . . among stakeholders with recognised expertise in the field of AI."[69] Whether impacted stakeholders end up with a seat on the Advisory Forum will depend on the degree to which lived

---

[64] *Id*.
[65] *Id*. at 96 (emphasis added).
[66] *EU AI Act Governance Structure and Supervisory Tasks - Inclusion of Stakeholders*, EUROPEAN CTR. FOR NOT-FOR-PROFIT L., (2022), https://ecnl.org/sites/default/files/2022-03/ECNL%20amendments%20AIA%20stakeholder%20engagement.pdf [https://perma.cc/35DU-SU9Q].
[67] EU AI Act, *supra* note 63, art. 67(2).
[68] See the reference to including civil society in the official webpage of the European Commission AI Office, https://digital-strategy.ec.europa.eu/en/policies/ai-office [https://perma.cc/DYV6-D2GD].
[69] *Id*. art. 67(3).

experience is framed and prioritized.

The AI Act also spurs the creation of voluntary codes of conduct that AI developers and deployers can eventually adopt. Among the objectives that the code of conduct model should reach, Article 95 mentions "facilitating an inclusive and diverse design of AI systems, including through the establishment of inclusive and diverse development teams and the promotion of stakeholders' participation in that process.[70] As we discuss further in Part II below, these provisions represent a nod to participatory design. The Act explains that stakeholders' participation should include relevant stakeholders such as "civil society organisations . . ., trade unions and consumer protection organisations in the design and development of AI systems," with attention to "diversity of the development teams, including gender balance."[71] To ensure that the voluntary codes of conduct are effective, the Act also recommends that "they should be based on clear objectives and key performance indicators to measure the achievement of those objectives. They should also be developed in an inclusive way, as appropriate, with the involvement of relevant stakeholders."[72]

C. US Examples: Data Privacy Laws, the NIST AI Risk Management Framework, the Executive Order on AI

In the United States, too, multiple proposed and newly enacted laws and guidance documents feature impacted stakeholder participation of varying modes and to varying degrees. We briefly review examples of both laws and guidance: data privacy laws, including the Colorado Privacy Act, the proposed federal American Data Privacy and Protection Act (ADPPA), and rules implementing the California Consumer Privacy Act; and guidance documents, such as the NIST AI Risk Management Framework (RMF) and President Biden's Executive Order on AI (which, to some degree, functioned as a hard law, too, governing executive agencies under the Biden administration).

Akin to the GDPR, the new rules promulgated by the Colorado Attorney General to implement the Colorado Privacy Act feature impacted stakeholder participation as an aspect of the "data protection assessment" process. The Colorado Privacy Act is an

---

[70] *Id*. art. 95(2)(d).
[71] *Id.* at 165.
[72] *Id*.

American-style general data protection law protecting the personal information of Colorado residents that passed in July 2021.[73] The state Attorney General was tasked with promulgating rules to implement the Act, which went into effect in July 2023.[74]

Under the new Colorado Privacy Act Rules, a "data protection assessment shall involve all relevant internal actors from across the Controller's organizational structure, and where appropriate, *relevant external parties*, to identify, assess and address the data protection risks."[75] The assessment itself shall include a list of "[r]elevant internal actors and *external parties* contributing to the data protection assessment."[76] This arguably creates documentation of whether such consultation occurred. While no reference is made specifically to impacted stakeholders, the Rules' language on "external parties" seems to echo the GDPR's language on involving impacted data subjects in the impact assessment process.

It is notable that the 2022 version of the repeatedly proposed (but not yet passed) federal data privacy law, the American Data Privacy and Protection Act (ADPPA), contains very similar scaffolding to the Colorado Privacy Act on impact assessments, which would also likely give rise to impacted stakeholder involvement should the law ever be enacted. Like Colorado's law, the ADPPA similarly tasked companies with conducting algorithmic impact assessments and the FTC with publishing guidance on how to implement those assessments.[77] The ADPPA required that companies include a "detailed description of steps the large data holder has taken or will take to mitigate potential harms from the covered algorithm to an individual *or group of individuals*, including related to. . . disparate

---

[73] By "American-style" we mean that it features both individual rights and some corporate responsibilities, built on the scaffolding of the Washington Privacy Act that never passed. It additionally applies to a more limited category of entities than, say, the GDPR, which is typical of American laws. *See* Anupam Chander, Margot E. Kaminski & William McGeveran, *Catalyzing Privacy Law*, 105 MINN. L. REV. 1733, 1747 (2021); *see also* Margot E. Kaminski, *Toward Stronger Data Protection Laws*, 68 Democracy: A Journal of Ideas (2023); Meg Leta Jones & Margot E. Kaminski, *An American's Guide to the GDPR*, 98 DENVER L. REV. 93, 106 (2021).

[74] COLO. REV. STAT. § 6-1-13 (2021).

[75] COLO. CODE REGS. § 904-3, R. 8.03 (2023) (emphasis added).

[76] *Id*. R. 8.04 (A)(16) (emphasis added).

[77] American Data Privacy Protection Act, H.R. 8152, 117th Cong. § 207(c)(1-4) (2022) [hereinafter ADPPA].

impact on the basis of individuals' race, color, religion, national origin, sex, or disability status."[78] Because of the parallels to the GDPR and the emphasis on harms to groups of individuals, we anticipate that if the ADPPA had been approved, a possible implementation would have also leaned on impacted stakeholder involvement in the assessment process.

California's Consumer Privacy Act (CCPA) is also likely to include impacted stakeholder input as part of its risk assessment process. Under that law, risk assessments are required for activities that present a significant risk to a consumers' privacy.[79] This will probably include enumerated activities such as using automated decisionmaking technology to make significant decisions concerning a consumer, to establish individual identity, or for physical or biological identification or profiling.[80] It may also include using personal data to train AI systems.[81]

As of this Article's initial drafting, the California Privacy Protection Agency (CPPA) had just begun the process of a new round of rulemaking. The agency released an early discussion draft of amendments to its rules on risk assessments in December 2023, and released the text of the proposed regulation in November 2024.[82] The proposed regulations envision that a "risk assessment may involve *external parties* to identify, assess, and mitigate the risks to consumers' privacy. These external parties may include, for example . . . a *subset of the consumers whose personal information the business seeks to process*; or stakeholders that *represent consumers' or others' interests,* including consumer advocacy organizations."[83]

While this consultation of external parties is seemingly permissive, an earlier discussion draft of the CCPA would have required businesses to explain why they have chosen not to consult external parties in preparation of a risk assessment, imposing at least

---

[78] *Id*. § 207(c)(1)(B) (emphasis added).
[79] Proposed CPPA Regulations, *supra* note 17 §7150(a) ("Every business whose processing of consumers' personal information presents significant risk to consumers' privacy as set forth in subsection (b) must conduct a risk assessment before initiating that processing.") [https://perma.cc/GX4A-FV3J].
[80] *Id*. §7150(b)(3-4).
[81] *Id*. §7150(b)(4).
[82] *See id.*
[83] *Id*. § 7151(b) (emphasis added).

an administrative burden for choosing not to do so.[84] And in its section on what must be included in risk assessments, the discussion draft appears to go further.[85] The draft states that, as part of the risk assessment process, "[a]t a minimum, the business shall consider the implementation of the following safeguards as appropriate . . . [c]onsulting the [aforementioned] *external parties* . . . at least every three years to ensure the business maintains current knowledge of emergent privacy risks and countermeasures, and using that knowledge to identify, assess, and mitigate risks to consumers' privacy."[86] Finally, the discussion draft requires that businesses include in a risk assessment or a separate internal document a list of "[r]elevant. . . *external parties* that have contributed to the risk assessment."[87] This suggests that the CPPA expects consultation with external parties, including impacted consumers and/or their representatives, to become par for the course in the risk assessment process.

Our next U.S. example is soft law, but influential soft law: the NIST AI Risk Management Framework. Unlike our other examples, this is not centralized top-down regulation. Rather, the AI Risk Management Framework is intended to serve as guidance, not be enforced by a regulator, and to evolve over time. However, it is likely to be influential in practice and may serve as the framework for later regulation in the United States.[88]

The NIST AI Risk Management Framework contemplates that a

---

[84] New Rules Subcommittee, California Privacy Protection Agency, Revised Draft Risk Assessment Regulations, § 7151(b)(1) (Dec. 2023) [hereinafter Discussion Draft CPPA Regulations], https://cppa.ca.gov/meetings/materials/20231208_item2_draft_redline.pdf [https://perma.cc/EY6D-5AP2] ("For the uses of automated decisionmaking technology or artificial intelligence . . . if the business has not consulted external parties in its preparation or review of the risk assessment, the risk assessment shall include a plain language explanation addressing why the business did not do so and which safeguards it has implemented to address risks to consumers' privacy that may arise from the lack of external party consultation.").

[85] *Id*. § 7152(a)(9).

[86] *Id.* § 7152(a)(9)(D) (emphasis added).

[87] *Id*. § 7152(a)(11) (emphasis added).

[88] See, e.g., Cameron F. Kerry, *NIST's AI Risk Management Framework Plants a Flag in the AI Debate*, BROOKINGS, Feb. 15, 2023, https://www.brookings.edu/articles/nists-ai-risk-management-framework-plants-a-flag-in-the-ai-debate/ [https://perma.cc/24L6-AG7N].

wide range of actors, including "potentially impacted individuals," can make important contributions to risk management practices.[89]

> These actors can assist in providing context and understanding potential and actual impacts; be a source of formal or quasi-formal norms and guidance for AI risk management; designate boundaries for AI operation (technical, societal, legal, and ethical); and promote discussion of the tradeoffs needed to balance societal values and priorities related to civil liberties and rights, equity, the environment and the planet, and the economy."[90]

More specifically, the AI Risk Management Framework suggests that depending on the "risk level of a particular AI system," companies should engage with "external collaborators, end users, *potentially impacted communities*, and others" in mapping the risks posed by an AI system.[91] The Framework further requires that "processes are in place for robust engagement with relevant AI actors," both internal and external.[92] The Framework suggests establishing "[f]eedback processes for end users and *impacted communities* to report problems and appeal system outcomes" and integrating this feedback "into AI system evaluation metrics."[93] In a nod to participatory design (discussed further in Part II below), the AI Risk Management Framework several times cites the importance of interdisciplinary and demographically diverse teams in "anchoring in design and development practices to user intentions and representatives of the broader AI community, and societal

---

[89] NIST, AI RISK MANAGEMENT FRAMEWORK (AI RMF 1.0) 10 (2023) [hereinafter NIST, AI RMF 1.0].
[90] *Id*. (cleaned up).
[91] *Id*. at 25 (emphasis added).
[92] *Id*. at 24 (requiring that "[o]rganizational policies and practices are in place to collect, consider, prioritize, and integrate feedback from those external to the team that developed or deployed the AI system regarding the potential individual and societal impacts related to AI risks.").
[93] *Id*. at 31*; see also id*. at 24 (requiring that "[m]echanisms are established to enable the team that developed or deployed AI systems to regularly incorporate adjudicated feedback from relevant AI actors into system design and implementation.").

values."[94]

Impacted stakeholders also made an appearance in President Biden's Executive Order on AI (Executive Order 14110). Issued in October 2023, the now-rescinded Executive Order on AI was directed primarily at federal agencies and established policy under the Biden administration for how the federal government would regulate its own use of AI systems.

Section 7 of the Biden Order addresses "[a]dvancing [e]quity and [c]ivil [r]ights." [95] In its discussion of the use of AI in determining and distributing government benefits, that section states that "agencies shall also consider opportunities to increase coordination, communication, and engagement about AI as appropriate with community-based organizations; civil-rights and civil-liberties organizations; academic institutions; industry; State, local, Tribal, and territorial governments; and other stakeholders."[96] The Executive Order refers to stakeholder engagement several other times.[97] One other notable example is in the section on protecting students. The Order requires the Secretary of Education to, within a year, "develop resources, policies, and guidance regarding AI. These resources shall address safe, responsible, and nondiscriminatory uses of AI in education, including the impact AI systems have on vulnerable and underserved communities, and shall be developed in consultation with stakeholders as appropriate."[98]

---

[94] *Id*. at 41; *s*ee also *id*. at 23 (requiring that "[d]ecision-making related to mapping, measuring, and managing AI risks throughout the lifecycle is informed by a diverse team (e.g., diversity of demographics, disciplines, experience, expertise, and backgrounds).").

[95] Exec. Order No. 14110, 88 FR 75191, 75211 (Oct. 30, 2023).

[96] *Id.* at 75212.

[97] *See e.g., id.* at 75214 (stating that in the name of ensuring transportation access for persons with disabilities, "the Architectural and Transportation Barriers Compliance Board is encouraged, as it deems appropriate, to solicit public participation and conduct community engagement."); *id.* at 75203 (requiring the Secretary of Commerce to "solicit input from . . . civil society, and other stakeholders through a public consultation process on potential risks, benefits, other implications, and appropriate policy and regulatory approaches related to dual-use foundation models").

[98] *Id.* at 75216.

II. Reasons for the Turn: Theoretical Arguments and Political Forces

The turn to impacted stakeholder participation thus has been a trend in recent policymaking in both the United States and the European Union. In this Part, we identify multiple reasons for this turn. We first discuss theoretical justifications for involving impacted stakeholders, especially representatives of historically marginalized communities. Then, we shift to an exploration of political forces. We identify a momentary alliance between proponents of neoliberal lighter-touch governance and proponents of bottom-up governance. This temporary alliance has implications for how impacted stakeholder participation has been crafted in recent laws.

A. Theoretical Explanations: Why Impacted Stakeholders?

We start with theoretical explanations for the turn to impacted stakeholder participation. First, the turn could constitute a response to calls for bottom-up governance of data-driven and AI systems. Second, it could constitute a response to calls for governance specifically for disproportionately impacted and historically marginalized persons and communities. Third, it could reflect privacy law's recent relational turn: a shift from understanding privacy in individualistic terms to conceptualizing privacy as collective and relational. Fourth, it could reflect the influence of "value-driven design" or "participatory design" practices. And fifth, it could be understood as an element of regulatory design, providing third-party accountability ("tripartism") to lighter-touch governance.

Theory matters greatly here. We disaggregate these explanations because we believe they *lead to calls for different kinds of interventions*. For example, a call for impacted stakeholder participation as a form of democratic governance can lead to attempts to design such participation to be loosely representative in nature. By contrast, a call for impacted stakeholder participation as part of "participatory design" focuses not on representation per se, but on structuring effective stakeholder feedback in the design process, and efficiently testing and improving a system through "design thinking." [99] In Part III, we return to the different

[99] Young, Magassa & Friedman, *supra* note 21, at 2.

implications of these five theoretical justifications for the law.

1. Democratic Participation

One way to understand the turn to impacted stakeholder participation is through the lens of democratic theory.[100] Through this lens, impacted stakeholder participation contributes to the advancement of democratic values, which are understood to be particularly threatened by regulated technologies.[101] These arguments connect to discussions of "throughput legitimacy:" the participation of affected individuals as direct participants in rule-setting organizations in service of institutional legitimacy.[102] They connect, too, to discussions of procedural justice: the idea that people view institutions that treat them with procedural fairness as more legitimate than those that do not.[103]

The democratic participation argument goes that impacted stakeholders should get to participate more directly in the governance of the technologies that impact them because this serves general democratic values of plurality, participation, equal representation, and non-discrimination.[104] This is all the more true

---

[100] Okidegbe, *supra* note 24, at 1705.

[101] There are multiple competing theories of democracy, but public participation is central to most. *See, e.g.,* Scott Skinner-Thompson, *Agonistic Privacy and Equitable Democracy*, 131 YALE L. J. FORUM 454, 465 (2021) ("Democratic theories may differ in terms of the emphasis they place on how and why participation matters, but they almost all agree that it does.").

[102] *See*, *e.g.*, Vivian A. Schmidt, *Democracy and Legitimacy in the European Union Revisited: Input, Output and 'Throughput,'* 61 POL. STUD. 2 (2013); Annalisa Volpato & Mariolina Eliantonio, *The Participation of Civil Society in ETSI from the Perspective of Throughput Legitimacy*, INNOVATION: THE EUROPEAN J. OF SOC. SCI. RSCH, Mar. 26, 2024, at 1.

[103] Tracey L. Meares, *Trust & Models of Policing*, 151 DAEDALUS 161, 163-64 (2022) ("Across institutional contexts (courts, businesses, schools), researchers have demonstrated consistent findings: public conclusions regarding legitimacy are tied more closely to judgments about the fairness of actions than to evaluations of the *fairness of outcomes* or the effectiveness of actors in achieving outcomes.") (emphasis added); *see also* TOM TYLER AND ALLAN LIND, THE SOCIAL PSYCHOLOGY OF PROCEDURAL JUSTICE 129-45 (1988).

[104] CHANTAL MOUFFE, THE RETURN OF THE POLITICAL 18-20 (1993) (referring to the need of radical democratic citizenship against oppression and towards a new impulse to democracy) ; Mireille Hildebrandt, *Privacy As Protection of the Incomputable Self: From Agnostic to Agonistic Machine Learning*, 20

because the technologies at issue (algorithmic decisionmaking, AI systems) are particularly prone to escaping effective democratic governance.[105] Michele Estrin Gilman, for example, justifies calls for public participation in the governance of data-driven systems by referring to the benefits of participatory governance in general.[106] She writes about the policy benefits of enabling more public participation by those most impacted by a technology.[107] Gilman argues that these benefits include improving the quality of governance, bolstering democratic legitimacy, improving accountability of both private and public actors, and broadening the social and cultural values considered during product design and testing.[108] These virtues reflect deliberative democracy's focus on governance through consensus-building and civic republicanism's conception of public participation as a check on government power.[109] Alexander Bhutan and Christian Fieleser similarly argue that the opacity of AI systems leads to uninformed decisions about AI governance—a problem which could be cured through engagement with experts and non-experts in different social studies

---

THEORETICAL INQUIRIES OF L. 83, 108 (2019); Kate Crawford, *Can an Algorithm be Agonistic? Ten Scenes from Life in Calculated Publics*, 41 SCI., TECH., & HUM. VALUES (SPECIAL ISSUE) 77, 77-78 (2016) (explaining that "political questions involve making a choice between conflicting options . . . not by reaching a rational consensus position but through a struggle between adversaries."). *See generally* Skinner-Thompson, *supra* note 101 (discussing the benefits of privacy in public for ensuring agonism in the public sphere by protecting marginalized individuals and groups).

[105] *See* Bloch-Wehba, *supra* note 20; Okidegbe, *supra* note 20, at 1705-07; Margot E. Kaminski, *Voices in Voices Out: Impacted Stakeholders and the Governance of AI*, 71 UCLA L. REV. DISC. 176, 180-81 (2024) (outlining general discussions of accountability and anti-democratic algorithms).

[106] Michele Estrin Gilman, *Beyond Window Dressing: Public Participation for Marginalized Communities in the Datafied Society*, 91 FORDHAM L. REV. 503, 522 (2022). Gilman also makes arguments that resonate more with what we call "participation equity," discussed in the next subsection.

[107] *Id*. at 523 ("At a societal level, public participation is said to enhance the quality of decision-making by including the perspectives of people most impacted by any given policy").

[108] *Id*.

[109] Jurgen Habermas, THE STRUCTURAL TRANSFORMATION OF THE PUBLIC SPHERE (Thomas Burger, trans., MIT Press 1991), 66. Skinner-Thompson, *supra* note 101, at 466 ("In contrast to deliberative democracy's emphasis on consensus building, . . . contestatory participation under a republican model underscores the role of participation aimed at the government itself (i.e., vertically).").

disciplines.[110]

Others have focused instead on agonistic pluralism, which emphasizes the centrality of ongoing contestation to a functioning democracy.[111] Kate Crawford and Mireille Hildebrandt each argue that algorithms, as complex and opaque technological artifacts, cloak and thus prevent potential moments of oppositional struggle in ways that are particularly threatening to a functional democracy.[112] They each theorize that the development and uses of these technologies are embedded with deep politics, subject to choices made largely in secret and largely in the private sector.[113] This lack of transparency threatens self-definition[114] (Hildebrandt) and forecloses potential sites of oppositional political struggle (Crawford).[115]

Impacted stakeholder participation can be understood, too, as a response to calls for bottom-up governance as a strong form of democratic participation. For example, Hannah Bloch-Wehba, in her calls for algorithmic governance "from the bottom up," argues for a "new vision for algorithmic accountability that places democratic participation at its center."[116] Bloch-Wehba advocates for a radical reconfiguration of algorithmic accountability, away from technocratic impact assessments and auditing and towards understanding and centering grassroots opposition efforts as governance, drawing on examples from social and racial justice and white-collar tech workers' movements. While the actual law of stakeholder participation charted here barely resembles Bloch-Wehba's vision, it can be understood as channeling such calls for bottom-up governance into law in a way more palatable to regulated companies and neoliberal regulators. Or, from a more critical perspective, it can be understood as an attempt to diffuse more radical democratic impulses.

---

[110] Alexander Buhmann and Christian Fieseler, *Deep Learning Meets Deep Democracy: Deliberative Governance and Responsible Innovation in Artificial Intelligence*, 33 BUS. ETHICS Q. 146, 150 (2022).
[111] Gilman, *supra* note 106, at 523-26.
[112] Hildebrandt, *supra* note 104, at 105-06.
[113] Hildebrandt, *supra* note 104, at 106; Crawford, *supra* note 104, at 82.
[114] Hildebrandt, *supra* note 104, at 105-06.
[115] Crawford, *supra* note 104, at 82.
[116] Bloch-Wehba, *supra* note 20, at 77.

As Okidegbe observes, the democratic participation argument tends to lead to calls for *participation for all*, instantiating in practices such as public hearings, or notice and public review.[117] Thus, the turn to impacted stakeholder participation might be characterized as just another avenue of democratic input alongside political process, public disclosure, and individual rights available to all. But as Okidegbe also notes, this presumes equal political power and access by all impacted groups—an assumption that she argues does not reflect current reality.[118]

2. Racial Justice, Anti-Discrimination, and Participation Equity

A number of laws, especially in the United States, refer to participation not just by impacted stakeholders in general but by historically marginalized groups and communities in particular.[119] This reflects calls for racial justice in algorithmic accountability. To distinguish these calls from more general calls for public participation, we refer to them here as calls for "participation equity."

On the one hand, laws that specifically reference participation by historically marginalized groups can be understood as a turn to incorporating "communal expertise" into lawmaking. [120]

---

[117] Okidegbe, *supra* note 20, at 1705-07, 1716.

[118] *Id.* at 1696, 1697.

[119] *See e.g.,* Colo. Rev. Stat. § 2-3-1707, XV stating that the AI task force should include "one member who represents disproportionately impacted communities"; see also Privacy Advisory Commission, About, CITY OF OAKLAND, https://www.oaklandca.gov/boards-commissions/privacy-advisory-board#page-about [https://perma.cc/VU2D-CF7P]. Okidegbe defines "oppressed groups" as "groups formed by virtue of a shared subordinated identity such as race, class, gender expression, gender identity, sexual orientation, or disability and the intersection thereof." Okidegbe, *supra* note 20, at 1710; *see also* THE DANISH INSTITUTE FOR HUMAN RIGHTS, CROSS-CUTTING: STAKEHOLDER ENGAGEMENT, HUMAN RIGHTS IMPACT ASSESSMENT GUIDANCE AND TOOLBOX (2020), at 27-28 [hereinafter HRIA Toolbox] ("Vulnerability . . . refers to being at a higher risk of being unable to anticipate, cope with, resist and recover from . . . adverse impacts. . . [and] can stem from an individual's status or characteristics (such as race, colour, sex. . .) or from their circumstances (such as poverty or economic disadvantage. . .)" (cleaned up)). *See also* GIANCLAUDIO MALGIERI, VULNERABILITY AND DATA PROTECTION LAW 49-51 (2023).

[120] *See*, *e.g.*, Okidegbe, *supra* note 20, at 1733 ("One concerns how to construct a

Communities, particularly marginalized communities, have lived experience of the harms that algorithms, AI, and other data-driven practices can inflict upon them. That lived experience can be valuable, the argument goes, for improving effective governance of such technologies and practices.[121] By valorizing lived experience as a form of expertise, it can more readily be prioritized alongside technocratic and technological expertise.[122]

But the characterization of experience as expertise is only part of the story, which more deeply speaks to injustices experienced by marginalized people that are exacerbated by the turn to algorithms and AI systems. As Okidegbe writes, general democratizing reforms responsive to calls based on general democratic participation theory "are not designed to address how state use of algorithms is anti-democratic to marginalized people" in particular.[123] They are not designed to make up for the ways in which algorithms themselves disproportionately are used upon, harm, and politically disempower oppressed groups. Per Okidegbe, generalized democratizing reforms "sidestep[] the structural dynamics that render transparency and deliberation on their own less valuable to oppressed groups than they may appear at first glance."[124] She explains that state uses of algorithms often serve to directly suppress democratic participation by marginalized groups; for example, signature-matching algorithms used in the electoral context and criminal punishment

---

commission in such a way that enables it to effectively blend communal, technocratic, and technological expertise within the institutional structure itself."); *id.* at 1739 ("[T]he hope is that this approach would facilitate a blending of communal, technocratic, and technological expertise."). Indeed, "ways of knowing by the state that support algorithmic use may be epistemically incompatible with communal ways of knowing oriented toward building a more equitable world." *Id.* at n.190). *See also* Gilman, *supra* note 106, at 523 (discussing the ways in which incorporation of feedback by marginalized groups in particular might improve governance outcomes).

[121] *But see* Ben Levin, *Criminal Justice Expertise*, 90 FORDHAM L. REV. 2777, 2829-30 (2022) (discussing the challenges with identifying which community members with lived experience hold the expertise to which policymakers should defer).

[122] *Id*.

[123] Okidegbe, *supra* note 20, at 1715. *See also id.* at 1728 ("Deliberative processes . . . operate on the presumption that all members of a polity have equal opportunity and equal voice to influence the state's use of algorithms . . . [which is] unattainable in practice.").

[124] *Id*. at 1726.

algorithms both result in disenfranchising members of Black and Brown communities, and other communities of color.[125] Gilman writes, too, of the ways in which the current U.S. political system devalues participation by poor people and marginalized people, justifying measures that increase their participation in the name of democratic values.[126] Throughout, Okidegbe echoes agonistic critiques, pointing out that algorithmic opacity forecloses potential sites of resistance especially for politically disempowered, marginalized groups.

Thus, Okidegbe and others call for what we term "participation equity" for oppressed groups.[127] From this perspective, public disclosure and governance by the political majority isn't equity.[128] Formal disenfranchisement and the foreclosure of sites of resistance justify close attention to existing and historic power imbalances in designing stakeholder input and participation. In its strongest form, calls for participation equity would entail not just allowing participation but establishing a "process by which oppressed groups can stop the technology's use."[129]

While Okidegbe writes of the use of algorithms by the state, many of the laws identified here would also govern private sector use. Indeed, laws that emphasize the participation of marginalized groups and communities reflect a growing awareness that data privacy policy raises anti-discrimination concerns.

---

[125] *Id*. at 1711.

[126] Gilman, *supra* note 106, at 526-27.

[127] *See also* Jessica M. Eaglin, *Constructing Recidivism Risk*, 67 EMORY L.J. 59, 66 (2017); Jessica M. Eaglin, *When Critical Race Theory Enters the Law & Technology Frame*, 26 MICH. J. RACE & L. 151, 161 (2021) (explaining that because "[algorithmic] tool construction is the production of social meaning . . . the demos should decide important questions of tool design. . . It calls for law to mediate the creation of social meaning, with a particular eye toward incorporating marginalized populations into that process."); HRIA Toolbox, *supra* note 119, at 27 (calling for "steps to identify and address discrimination, vulnerability and marginalisation in engagement processes" since "individuals may have particular characteristics that warrant attention and protection.").

[128] Okidegbe, *supra* note 20, at 1723 ("Legislative bodies are deeply underrepresentative and unresponsive to the needs of oppressed groups.") "Though deliberative processes may lead to bans of the algorithmic technologies that infringe the rights of the majority . . . they will rarely translate into bans on algorithmic technologies that target oppressed groups specifically." *Id*. at 1729.

[129] Okidegbe, *supra* note 20, at 1721 and 1734 (calling for veto power in community governance of carceral algorithms).

Scott Skinner-Thompson has written on privacy as a tool for antisubordination, [130] a way of preserving necessary space for agonistic pluralism in the physical and digital public sphere.[131] It is also now well accepted that data processing can produce disparate impacts both by reproducing historical biases and by cloaking outright discrimination.[132] In the United States, some advocate for addressing such discrimination through data privacy law and regulations,[133] while others debate just how far data privacy law and institutions should intervene in the realm of civil rights institutions historically tasked with addressing discrimination.[134] What is clear is that antidiscrimination goals and norms are making their way into data privacy law.[135] That is, impacted stakeholder participation is the process part of data protection's recent substantive attempts to address bias, unfairness, and discrimination.[136]

Color-blind and gender-blind privacy law can fail to protect the most vulnerable. [137] In the data privacy context, Anita Allen describes what she terms the "Black Opticon": African Americans' "disparate online vulnerability."[138] She charts the ways in which

---

[130] *See generally* SCOTT SKINNER-THOMPSON, PRIVACY AT THE MARGINS (2020).
[131] Skinner-Thompson, *supra* note 101.
[132] Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CALIF. L. REV. 671, 685, 692-93 (2016); Tiffany Li, *Privacy and/as Civil Rights*, 36 BERKELEY TECH. L.J. 1265, 1275 (2021).
[133] Andrew Selbst & Solon Barocas, *Unfair Artificial Intelligence: How FTC Intervention Can Overcome the Limitations of Discrimination Law*, 171 U. PA. L. REV. 1023, 1091-92 (suggesting that the FTC address such discrimination through data privacy law and regulations); Samantha Lai & Brooke Tanner, *Examining the Intersection of Data Privacy and Civil Rights*, BROOKINGS (Jul. 18, 2022), https://www.brookings.edu/blog/techtank/2022/07/18/examining-the-intersection-of-data-privacy-and-civil-rights [https://perma.cc/Q3DU-KSXJ].
[134] *See*, *e.g.*, Cameron F. Kerry et al., *Bridging the Gaps: A Path Forward to Federal Privacy Legislation*, BROOKINGS, June 3, 2020, at 14 (arguing that "[p]rivacy legislation should not alter existing federal or state anti-discrimination laws, and the agencies currently tasked with anti-discrimination enforcement (e.g., the EEOC) should maintain their primary roles."), https://www.brookings.edu/wp-content/uploads/2020/06/Bridging-the-gaps_a-path-forward-to-federal-privacy-legislation.pdf [https://perma.cc/47Z8-NCHX].
[135] *See*, *e.g.*, Andrew D. Selbst, *An Institutional View of Algorithmic Impact Assessments*, 35 HARV. J. OF L. AND TECH. 117 (2021).
[136] GDPR, *supra* note 14, recital 71.
[137] *See generally* Allen, *supra* note 19. *See also* Mary Anne Franks, *Democratic Surveillance*, 30 Harv. J. L. & Tech. 425, 441-49 (2017).
[138] Allen, *supra* note 19, at 913.

data surveillance and data processing exploit Black people through "(1) multiple forms of excessive and discriminatory surveillance; (2) targeted exclusion through differential access to online opportunities; and (3) exploitative online financial fraud and deception."[139] Allen calls for "shap[ing] law and legal institutions that will better serve African Americans' platform-governance-related interests no less than, and along with, the interests of others."[140]

Privacy as anti-discrimination is not solely about arriving at particular substantive law, but also about changing the process through which policies are decided and technologies are designed and deployed. For example, Allen writes that "[d]igital-privacy and data-protection law proposals fashioned to promote equitable governance online must be responsive to calls for improved online governance made *by and on behalf of* African Americans relating to these forms of pervasive and persistent disadvantage."[141] Writing of education privacy, Fanah Gamal argues that the law's failures "harm[] an array of communities" and that addressing "[b]oth the privacy and equality dimensions of [these] failures will require frequently siloed areas of law and advocacy. . . to explicitly name their overlapping interests and common threats."[142] Gamal calls not just for transparency in general but for empowering "organized collectives" to "push for more egalitarian educational environments."[143] These calls for not just substantive but procedural interventions reflect the growing critical literature on policing and mass incarceration that calls for returning power to the communities most affected by these practices.[144]

---

[139] *Id.* at 910.
[140] *Id*. at 913.
[141] *Id*. at 910 (emphasis added).
[142] Fanah Gamal, *The Private Life of Education*, 75 STAN. L. REV. 1315, 1359 (2023).
[143] *Id*. at 1363.
[144] *See also* Amna A. Akbar, *Toward a Radical Imagination of Law*, 93 N.Y.U. L. REV. 405 (2018); Jocelyn Simonson, *Police Reform through a Power Lens*, 130 Yale L.J. 778, 787 (2021); Dorothy E. Roberts, *Democratizing Criminal Law as an Abolitionist Project*, 111 NW. U. L. Rev. 1597 (2017).

3. Privacy's Shift from the Individual to the Collective and Relational

Calls for democratic accountability also resound in and are paralleled by a recent and marked shift in the privacy literature. Data protection is centrally concerned with using accountability to check otherwise unchecked power and correct power imbalances. Historically, data protection laws have largely attempted to do so by affording individuals some form of control.

However, in recent years there has been mounting criticism of just how effective individual rights can be, and of how well an individualized conception of data really tracks data practices and corresponding harms.[145] The turn to impacted stakeholder participation can be characterized within this intellectual lineage as an attempt to institute a "mesosystemic layer" of governance practices: between individual governance and top-down societal level (macrosystemic) governance.[146]

Shelly Kreiczer-Levy has, for example, recently identified the "data crowd" as an essential stakeholder of the data economy. She defines the "data crowd" as unorganized stakeholder of the data economy that is unable to form an agenda but is both dependent on the other individuals of the same crowd (interdependency) and on the power of an external authority (social media platforms, AI deployers, data controllers).[147] Kreiczer-Levy argues that these "crowds" share uniform interests and similar situations of power imbalances that should justify a valorization of their collective nature, rather than the individualistic protection that they receive now.[148]

To be clear, data privacy scholarship has long emphasized the

---

[145] Viljoen, *supra* note 12, at 598-600; McNealy, *supra* note 13 at 525 ("[D]ata is not singular, but always comes attached with labels, contexts, and biases fastened from its inception, if not collection. . . This view also requires a different strategy for governance – one that acknowledges data's nature and networked existence, and moves beyond the individualistic, consent-based current models.").

[146] McNealy, *supra* note 13 at 535 ("[T]he mesosystem [is] a system of microsystems. . . [T]his would mean examining both the connections that data has with other kinds of data as well as the attachments and labels connected with the data. The mesosystem also encompasses all of the structures or settings that shape data over the life cycle.").

[147] Shelly Kreiczer-Levy, *The Data Crowd as a Legal Stakeholder*, 44 OXFORD J. OF LEGAL STUD. 645, 648-49 (2024).

[148] *Id*. at 666-67.

collective aspects of data privacy, especially its implications for democracy.[149] This justifies governance of privacy at the layer of society writ large.[150] The trend of incorporating impacted stakeholders or their representatives directly into regulation can be understood as instantiating this shift, both as a way of more directly representing collective and group harms, and as a way of searching for some other means than individual rights of checking the power of data controllers.

The academic literature in privacy law scholarship has long centered the concept of power imbalance. According to Daniel Solove,[151] privacy can act as a counterbalance to power disparities, particularly between individuals and government organizations. Julie Cohen examines privacy, surveillance, and self-disclosure from the perspective of relational power,[152] while Lisa Austin compares the harm paradigm and the power paradigm in the realm of privacy.[153] Austin suggests that privacy be reconsidered as a tool for rebalancing power dynamics, with a focus on "power-over" (a

---

[149] See, e.g., Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1613–14 (1999) (exploring the "inadequacies of the traditional liberal understanding of information privacy, which views privacy as a right to control the use of one's personal data . . . [and] argu[ing] that information privacy is best conceived of as a constitutive element of civil society."); Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1912 (2013) ("Conditions of diminished privacy . . . impair the practice of citizenship. . . [A] liberal democratic society cannot sustain itself without citizens who possess the capacity for democratic self-government.")

[150] See, e.g., Gilman, *supra* note 106, at 526. Viljoen, *supra* note 12; Solow-Niederman, *supra* note 12; Neil Richards and Woodrow Hartzog, *A Relational Turn for Data Protection?*, 6 EUROPEAN DATA PROTECTION L. REV. 492 (2020). *See also* Gilman, *supra* note 106, at 525, discussing CARISSA VÉLIZ, PRIVACY IS POWER 80–81 (2021); Joan Donovan, *Deconstructing Disinformation's Threat to Democracy*, 44 FLETCHER F. WORLD AFFS. 153, 153 (2020); Darakhshan J. Mir, *Designing for the Privacy Commons*, *in* GOVERNING PRIVACY IN KNOWLEDGE COMMONS 245 (Madelyn Rose Sanfilippo, Brett M. Frischmann & Katherine J. Strandburg eds., 2021); VIRGINIA EUBANKS, AUTOMATING INEQUALITY: HOW HIGH-TECH TOOLS PROFILE, POLICE, AND PUNISH THE POOR 12 (2018).

[151] Daniel J Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1399 (2001).

[152] JULIE E. COHEN, CONFIGURING THE NETWORKED SELF 127-52 (Yale Univ. Press 2012). *See also* Julie E. Cohen, *Turning Privacy Inside Out*, 20 THEORETICAL INQUIRIES IN L. 22 (2019) (on the link between privacy and power).

[153] Lisa Austin, *Enough About Me: Why Privacy Is About Power, Not Consent (or Harm), in* A WORLD WITHOUT PRIVACY: WHAT LAW CAN AND SHOULD DO? 189 (Austin Sarat ed., 2014).

spatial power that constrains public power, particularly in the field of surveillance) and "power-to" (empowering individuals to take actions that would otherwise be impossible).[154] Ryan Calo also considers this conceptualization of privacy in terms of power.[155] He sees privacy as a means of mitigating vulnerability, based on his theory that power imbalance analysis is fundamental to understand privacy harms.[156] Similarly, one of us has identified the EU data protection legal framework as a tool to contrast the structural link between digital vulnerability suffered by data subjects and power imbalance of dominant data controllers.[157]

The connection between data privacy, power, and vulnerability is crucial. Hildebrandt notes that power in the digital realm is a "framing power" that can reconfigure choice architectures in line with whoever pays for them.[158] Digital companies can use abusive and unfair choice architectures as tools to force customers to accept undesirable data processing conditions in exchange for the use of a specific digital platform.[159]

Similarly, Pettit defines power through his theory of "domination."[160] He describes it as the situation where a subject/entity (the dominator, the "powerful") has the capacity to interfere on an arbitrary basis in certain choices that the other (the dominated, the "powerless") can make. This analysis can be easily applied to the world of digital technologies and dominant big tech platforms, which interfere with consumers' choices and daily life through a dense structure of explicit or subliminal incentives. A distinguishing characteristic of Pettit's dominance theory is the arbitrariness through which the dominator may interfere with the dominated.[161] According to him, to prevent this arbitrariness, we

---

[154] *Id.*

[155] Ryan Calo, *Privacy, Vulnerability, and Affordance*, 66 DEPAUL L. REV. 591, 601 (2017).

[156] *Id.* at 598. *See also* Daniella DiPaola & Ryan Calo, Socio-Digital Vulnerability at 2 (Jan. 7, 2024) (unpublished manuscript), https://ssrn.com/abstract=4686874 [https://perma.cc/EQH2-2UZ2].

[157] MALGIERI, *supra* note 119, at 234-35.

[158] Mireille Hildebrandt, *The Issue of Bias: The Framing Powers of ML, in* MACHINE WE TRUST: PERSPECTIVES ON DEPENDABLE AI 52, 56 (Marcello Pelillo & Teresa Scantamburlo eds., 2021).

[159] *Id.*

[160] PHILIP PETTIT, REPUBLICANISM: A THEORY OF FREEDOM AND GOVERNMENT 56-79 (Oxford Univ. Press 1999).

[161] *Id.* at 56.

should create clear and solid procedures to "track the interests" (the welfare, the wellbeing) of the powerless parties, e.g., through their representatives and through accepted rules.

The problem of domination and power imbalances—especially in the design of AI systems and data processing activities—is connected to the underrepresentation of marginalized minorities in key decision-making. An interesting analysis is offered by "standpoint theory"/standpoint epistemology. According to this theory, knowledge is created through the power dynamics that shape and divide social groups into dominant and non-dominant categories.[162] The experiences of individuals within these categories result in unequal opportunities, leading to distinct ways of knowing and being. Proponents of standpoint theory argue that non-dominant group members can offer a more complete understanding of reality because they have lived it from both perspectives. Recently, Kirsten Martin has applied this theory to business ethics, focusing on the link between underrepresentation and standpoints in Big Tech's decision-making.[163] Traditional diversity engagement solutions based on standpoint epistemology have been criticized because of deference mechanisms in which only the most privileged representatives of marginalized and impacted individuals are involved.[164] Rediscussing participatory methodology may thus be crucial.[165]

All of these burgeoning discussions of relationality and vulnerability arguably have led to a shift in data privacy laws: from individual control to increased stakeholder participation. Historic privacy and data protection laws, best practices, and codes of conduct have generally relied on the "notice-consent-contest" approach. According to this model, the best way to protect rights and participation of individuals in complex data processing

---

[162] Brenda J. Allen, *Standpoint Theory*, The International Encyclopedia of Intercultural Communication (Dec. 13 2017).

[163] Kirsten Martin, 2022 Society for Business Ethics Presidential Address 6-8 (2022), https://kirstenmartin.net/wp-content/uploads/2022/10/BEQ-Presidential-Address-Who-Counts-in-Business-Ethics-10-18-SUBMIT.pdf [https://perma.cc/U5H7-RUYZ].

[164] *See e.g.*, Olúfẹ́mi Táíwò, *Being-in-the-Room Privilege: Elite Capture and Epistemic Deference*, 108 THE PHILOSOPHER 61 (2020).

[165] Indeed, some academics are turning to this now. *See*, *e.g.*, Flora Cornish, *Participatory Action Research*, in 3 NATURE REVIEWS METHODS PRIMERS 1 (2023).

activities is to (a) inform them that their data are being processed and (b) to ask for their consent to such processing or, (c) potentially, to allow them to contest the automated decision ex-post and request a new human-mediated decision after they have expressed their own view.[166] This model is statutorily dominant both in the EU and the United States. When rolling out data projects, business enterprises are usually legally obliged or at least committed to informing affected people, asking for their consent, and/or offering them remedial ex-post action in the case of a violation of their rights.[167]

Here, the communication between different parties (for example, employer vs. employees, corporate management vs. stakeholders) is generally based on an adversarial design model, generating "a condition of forever looping contestation."[168] Such loops of contestation have been welcomed in data projects because they are seen as a first step of constructive technology assessment[169] that could lead to pluralism in design practices. [170]

The notice-consent-contest model is inspired by the principle of data self-determination and autonomy of individuals. This model, as implemented by data protection legislation across the world, gives great importance to transparency and privacy policy disclosures. The model is based on the underlying neoliberal assumption that the data subject may exercise their rights autonomously. Past scholarship has argued that the emphasis on free and informed consent in data protection law and social responsibility standards draws from a theoretical understanding of consent as an "autonomous authorization model,"[171] as developed by Faden and Beauchamp.[172] Such a model generally assumes our right as rational human beings to choose our course of action freely and it is reflected in our ability to consent.

The consent-contest model has, however, proven ineffective for

---

[166] Solon Barocas & Helen Nissenbaum, *On Notice: The Trouble with Notice and Consent*, 7 in PROC. OF THE ENGAGING DATA F.: THE FIRST INT'L F. ON THE APPLICATION AND MGMT OF PERS. ELECTRONIC INFO. (2009).

[167] Richard Warner & Robert Sloan, Beyond Notice and Choice: Privacy, Norms, and Consent, *J. High Tech. L*. (2013).

[171] *Id.*

[171] *Id.*

[171] *Id.*

[171] *Id.*

[172] *See generally* RUTH R. FADEN & TOM L. BEAUCHAMP, A HISTORY AND THEORY OF INFORMED CONSENT (1986).

many reasons. The autonomous authorization model of a data subject capable of making a free, conscious, and rational decision to consent based on the available information may have been overemphasized. First, information notices might be fallacious, and individuals might be either uninterested in or incapable of understanding real risks and implications of data processing activities.[173] In addition, in many contexts—and especially in the digital ecosystem—there is no real freedom to give or deny consent, either because there is no real alternative or because of a power imbalance between the customer and the service provider.[174] Moreover, many individuals are unaware that they belong to an especially vulnerable category; for example in the case of people subject to affinity profiling,[175] discrimination, or other adverse effects, e.g., digital addiction or price discrimination.[176] This means that even well-informed individuals might be unable to react (through consent provision/denial or through contestation) to unfair processing of their data.

Network effects and digital lock-in exacerbate the power imbalance between big tech companies and consumers, and facilitate framing of consumers' choice sets in ways more favorable to the service provider.[177] Even if we might have personal resistance to giving our consent to data processing, and even if there is no brute force imposing on us to give consent, market and technological

---

[173] *See* Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1880-81 (2013) (explaining that "cognitive problems impair individua's ability to make informed, rational choices about the costs and benefits of consenting to the collection, use, and disclosure of their personal data."); Schermer et al., *supra* note 171, at 171 (explaining that "data subjects do not fully contemplate the consequences and risks of personal data processing . . . [and] simply consent whenever confronted with a consent request"); Gabriela Fortuna-Zanfir, *Forgetting about Consent. Why the Focus Should Be on "Suitable Safeguards" in Data Protection Law, in* RELOADING DATA PROTECTION: MULTIDISCIPLINARY INSIGHTS AND CONTEMPORARY CHALLENGES 237-44 (Serge Gutwirth, Ronald Leenes & Paul De Hert eds., 2014).

[174] AUSTIN, *supra* note 153, at 161; Benjamin Bergemann, *The Consent Paradox: Accounting for the Prominent Role of Consent in Data Protection*, *in* PRIVACY AND IDENTITY MANAGEMENT. THE SMART REVOLUTION 115 (Eleni Kosta, Igor Nai-Fovino, Marit Hansen, Simone Fischer-Hübner eds., 2018).

[175] Sandra Wachter, *Affinity Profiling and Discrimination by Association in Online Behavioral Advertising*, 35 BERKELEY TECH. L.J. 367, 403 (2020).

[176] Barocas & Selbst, *supra* note 132, at 677-92.

[177] Neil Richards and Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 WASH. U. L. REV. 1461, 1463, 1466 (2019).

architecture make us act in the way that our powerful counterparts prefer. As Véliz noted, power, like energy, can transform itself from one kind to another.[178] For example, market power can become knowledge power.[179] Customers will accept giving more personal data to platforms, which could create an increasingly personalized environment where the user is more easily nudged to accept new requests for personal data and so on in a vicious cycle.

Scholars in gender studies, data colonialism, and data justice[180] have pointed out the underrepresentation of many stakeholders in the design of data-driven business models renders their ex-post consent declaration meaningless: a "take-it-or-leave-it" exercise rather than an expression of will that could effectively influence the design and implementation of data projects.[181] This observation is supported by a study conducted by France's Commission Nationale Informatique et Liberté (CNIL), which found that data subjects who lodged complaints to Data Protection Authorities were mostly men, with good education, income level, and social position.[182] It is plausible that this problem of underrepresentation is not limited to who lodges formal complaints to the regulators, but also concerns who denies consent, who objects to data processing activities, and who contests automated decisions. As many feminist scholars have argued, the informed consent model is based on a neoliberal approach that tends to disregard societal inequalities and aims to

---

[178] CARISSA VÉLIZ, PRIVACY IS POWER: WHY AND HOW YOU SHOULD TAKE BACK CONTROL OF YOUR DATA 65 (2020).

[179] *Id.*

[180] *See generally* Joana Varon & Paz Peña, *Artificial Intelligence and Consent: A Feminist Anti-Colonial Critique*, 10 INTERNET POL. REV. 2 (2021); Nick Couldry & Ulises A Mejias, *Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject*, 20 TELEVISION & NEW MEDIA 336 (2019); Silvia Masiero & Soumyo Das, *Datafying Anti-Poverty Programmes: Implications for Data Justice*, 22 INFO., COMM. & SOC. 916 (2019).

[181] Claudia Quelle, *Not Just User Control in the General Data Protection Regulation, in* PRIVACY AND IDENTITY MANAGEMENT. FACING UP TO NEXT STEPS 4 (Anja Lehmann, Diane Whitehouse, Simone Fischer-Hübner, Lothar Fritsch & Charles Raab eds., 2017).

[182] *Le plaignant type? Un homme, diplômé et cadre*, LABORATOIRE D'INNOVATION NUMERIQUE DE LA CNIL (Feb. 25, 2022), https://linc.cnil.fr/fr/le-plaignant-type-un-homme-diplome-et-cadre [https://perma.cc/Z5V6-WCHN].

limit states responsibility to protect consumers.[183] These disadvantages and dysfunctions can be disproportionately harmful for social groups that are already vulnerable.[184]

According to Pettit's theory on domination, consent is not a sufficient guard against arbitrariness of dominators, mostly because of power asymmetries that do not allow individuals either to perceive the risk of giving consent or to feel free to deny consent.[185] Rather than relying upon consent, powerless individuals can be guaranteed the permanent possibility of effectively contesting power and sharing their interests and ideas to drive the decisions impacting them.[186] This can be realized through specific procedures where the representatives of powerless subjects express their interests and goals. Participatory decision-making (at any level) can be an effective way to mitigate power asymmetries and overcome the limits of consent or paternalism.

4. "Value Sensitive Design" and "Participatory Design" Practices

In sum, there has been a growing recognition of the limitations of consent as a mechanism to protect individual rights in the context of data-driven systems, particularly those involving AI. In particular, the communication between different parties (for example, employer vs. employees, corporate management vs. stakeholders) is generally based on an adversarial design model, generating "a condition of forever looping contestation." Such loops of contestation have been welcomed in data projects because they are seen as a first step of constructive technology assessment that could lead to pluralism in design practices.

Loops of contestations are constructive technology design and assessment only if different stakeholders had equal power and similar objectives—but the notice-consent-contest model does not prevent different stakeholders from having different informational

---

[183] *See* Martha Albertson Fineman, *Vulnerability and Inevitable Inequality*, 4 OSLO LAW REVIEW 133, 134 n.1 (2017).

[184] *See* Gianclaudio Malgieri & Jedrzej Niklas, *The Vulnerable Data Subjects: A Gendered Data Subject?*, 37 COMPUT. L. & SEC. REV. 1, 15 (referring to the limits of the neoliberal approach for what concerns the protection of vulnerable data subjects).

[185] Philip Pettit, *Liberty as Non-Domination*, in REPUBLICANISM: A THEORY OF FREEDOM AND GOVERNMENT 62 (1999).

[186] *Id*. at 56–59.

and structural power, different levels of understanding of the technological systems, and very different contractual power in negotiating new terms and rules. This often turns into counterproductive adversarial approaches incapable of mitigating power imbalances suffered by vulnerable groups.

As a result, there has been a shift towards greater involvement of impacted stakeholders in both the design and governance of these systems.[187]

This approach seeks to address the power imbalances inherent in many AI systems, which can result in marginalized groups being disproportionately impacted by algorithmic decision-making.

Involving diverse stakeholders, including those who experience higher forms of vulnerability in a specific digital context, in the development process arguably can contribute to more inclusive, fair, transparent and accountable AI and digital systems.[188] In particular, engaging diverse stakeholders in decision-making and preliminary impact assessments can lead to better anticipation and mitigation of the risks to fundamental rights (e.g., discrimination, manipulation, stigmatization). Moreover, participatory approaches can empower vulnerable individuals by giving them a voice in the development of AI and digital systems.

But what does it mean to take a participatory approach to data governance and the governance of data-driven algorithms? Participatory design theorists[189] emphasize the notion of "design thinking:" an "approach to the design of technology . . . throughout the design process."[190] "Design thinking" is different from democratic participation and from anti-discrimination, though it too may be driven by a pursuit of racial justice. It is concerned with an iterative process of system design[191] that emphasizes not comprehensive society-wide analysis but "envisioning alternatives to current conditions that, in both large and small ways, improve" the end product, whether that be technology itself or surrounding

---

[187] SASHA COSTANZA-CHOCK, DESIGN JUSTICE: COMMUNITY-LED PRACTICES TO BUILD THE WORLDS WE NEED 18 (2020).

[188] Eduard Fosch-Villaronga & Hadassah Drukarch, *Accounting for Diversity in Robot Design, Testbeds, and Safety Standardization*, 15 INT'L J. SOC. ROBOTICS 1871, 1882-83 (2023).

[189] *Id.* at 2.

[190] *Id*. at 2.

[191] *Id*. at 3 ("an artifact (e.g., system design) emerges through iterations upon a process that is more than the sum of its parts.").

policy. [192]

Value Sensitive Design, as one example, queries what values are implicated in the design process and how one should engage in trade-offs, with an eye to which stakeholders are affected.[193] It is not necessarily concerned with representation in the democratic sense of the term. The Diverse Voices method, one subcategory of Value Sensitive Design coined at the University of Washington Tech Policy Lab, "aims to surface some but not all problems associated with an artifact . . . in order to make improvements. There is no claim to surface all problems from all perspectives, nor to produce generalizable knowledge."[194] The goal is *resource-efficient improvement*, not democratic representation.[195]

Again we see reference to "experiential expertise," with community members described as "experiential experts" who have "lived experience as a member of a particular group." [196] The Diverse Voices method outlines three kinds of experts: technical experts, policy experts, and "experiential experts comprised of diverse stakeholder groups whose lives will likely be substantively affected by the way a given technology will be instituted in society through policy."[197]

Other versions of value-sensitive design emphasize the import of hiring and involving diverse employees.[198] But this can lead to

---

[192] Young, Magassa & Friedman, *supra* note 21 at 90 ("Design thinking approaches make progress by envisioning alternatives to current conditions that, in both large and small ways, improve situations, circumstances, or experiences (Cross 1982; Nelson and Stolterman 2012). Rather than conducting comprehensive analyses of the type often associated with social-scientific approaches (e.g. Dryzek et al. 2009; Fung 2003), design thinking approaches can offer targeted insights about artifacts-in-progress that lead to improvement.").

[193] *Id*. at 92.

[194] Lassana Magassa, Meg Young, & Batya Friedman; *Diverse Voices: A How-To Guide for Facilitating Inclusiveness in Tech Policy*; Tech Policy Lab, University of Washington (2017).

[195] *Id*. ("Rather, the more modest goal is to leverage the views of a relatively small number of experts to improve the overall quality of a given artifact. We employ a design thinking approach because it is resource-efficient and we believe it can be effective.").

[196] *Id.* at iii (Key Terms). Young et al, *supra* note 21, at 90 ("we use the term experiential expert to refer to people who are living the experience or those closely associated with someone living the experience (e.g., family members, institutional advocates).").

[197] *Id.*

[198] COSTANZA-CHOCK, DESIGN JUSTICE, *supra* note 21, at 72.

overburdening marginalized employees, and to a lack of understanding that one member of a marginalized or oppressed group does not necessarily speak for a community—or that communities consist of diverse perspectives. In addition, a simple diversification of employment is not the solution to intersectional and structural inequality, especially considering that the focus should be on diverse *users,* where users tend to be assumed to be members of the dominant privileged groups.[199]

The legal turn to impacted stakeholder participation often obviously reflects calls for participatory design. In the impact assessment process, it reflects the notion of embedding stakeholder values into technological design at the design stage. But as with participatory design in general, the legal version of participatory design risks participation washing. It also could be characterized as describing what many companies are already doing: incorporating some version of value-sensitive design into the design process.

Building on value-sensitive design and on existing mechanisms for both individual and community participation in algorithmic design systems,[200] Sasha Costanza-Chock proposes a manifesto for "design justice," recommending user-centered and group-centered practices aimed at combatting structural inequality in the design of data technologies. The starting point is to question the neoliberal power matrix of domination inherent in the business decision-making of tech companies and acknowledge structural inequalities, based on intersectional discrimination towards marginalized communities.[201] This objective does not require only diversity in the design process, but participatory approaches engaging with different contextual (users') community realities and a redefinition of design education and tech business narratives. Participatory practices in design justice requires implementing new codesign methodologies, developing specific concrete mechanisms for community

---

[199] *Id.* at 75-78.

[200] *Id.* at 85; Judith Gregory, *Scandinavian Approaches to Participatory Design* 19 INT'L J. ENG'R EDUC. 62 (2003). *See also* ActionCatalogue, https://actioncatalogue.eu/ (accessed June 1, 2025) (a catalogue of possible participatory design initiative,); Algorithmic Justice Leage, *CRASH Project, Formerly Algorithmic Vulnerability Bounty Project (AVBP)*, https://www.ajl.org/avbp> (accessed June 1, 2025) (addressing vulnerable subjects' participation in order to prevent algorithmic-driven harms).

[201] COSTANZA-CHOCK, DESIGN JUSTICE, *supra* note 21, at 20-22.

accountability and centering community "needs" over tools (anticipating impacts and checking preferences), investing in education both formal and informal that teaches codesign methods to more practitioners, creating tech clinics modeled on legal clinics, and avoiding "parachuting technologists into communities."[202]

5. Regulatory Design

Finally, impacted stakeholder participation can act as a check on industry capture of regulatory bodies, and establish accountability to (or in spite of) soft-touch collaborative government regulation. It can be understood as an element of "tripartism:" the empowerment of third-party voices in governance, towards both accountability and capacity-building.[203]

As one of us has charted at length, the new Law of AI leans heavily on risk regulation.[204] This approach tasks companies and government agencies with identifying and mitigating systemic risks that include unfairness, bias, and discrimination, in conjunction with privacy harms to both individuals and to groups. Such regulation tends to draw on long-standing practices in data protection law of delegation to the private sector.[205]

Tasking companies with partially regulating themselves creates the obvious potential for, and often actuality of, capture. One oft-cited way to mitigate this problem is what Ian Ayres and John Braithwaite refer to as "tripartism:" bringing in third parties as regulatory force multipliers to help check both self-interested behavior by regulated entities and capture of under-resourced regulators.[206] Algorithmic accountability laws frequently lean on third-party auditors and expert bodies. Impacted stakeholder groups can be understood as additional self-interested voices to amplify tripartism and target it at protecting those to whom risks accrue.

---

[202] *Id.* at 98-99. See also Lisa M. Vaughn & Farrah Jacquez, *Participatory Research Methods – Choice Points in the Research Process*, 1 J. OF PARTICIPATORY RSCH. METHODS 1 (2020).

[203] AYRES & BRAITHWAITE, RESPONSIVE REGULATION, *supra* note 54; Ayres & Braithwaite, *Tripartism*, *supra* note 54.

[204] Kaminski, *The Developing Law of AI*, *supra* note 24.

[205] KENNETH A. BAMBERGER & DEIDRE K. MULLIGAN, PRIVACY ON THE GROUND: DRIVING CORPORATE BEHAVIOR IN THE UNITED STATES AND EUROPE (MIT Press 2024); Kaminski, *Binary Governance*, *supra* note 54.

[206] AYRES & BRAITHWAITE, RESPONSIVE REGULATION, *supra* note 54; Ayres & Braithwaite, *Tripartism*, *supra* note 54.

The kind of risk regulation being deployed in this space tends to center less on public accountability, and more on tasking companies with conducting enterprise risk management.[207] Enterprise risk management is when companies use internal processes to evaluate and manage risks *to themselves*, just as companies might evaluate and mitigate financial risks or other sorts of liability. Stakeholder participation in risk management in theory forces companies to consider risks *to others*. It potentially serves as one way to bring countervailing external voices into the process to broaden the lens and contest myopic definitions of harms.

B. Political Forces

The above explanations offer us theories as to why we *should* have impacted stakeholder participation. They do not necessarily offer pragmatic explanations as to *why*, in practice, these provisions are making their way into the law.

On the one hand, lawmakers are almost certainly considering the harms AI and other algorithms inflict on marginalized groups. This is a response to effective public framing of algorithmic and AI harms. The motivating paradigmatic narratives for regulating AI are about racist risk assessments that disproportionately harm Black men, and racist and sexist facial recognition algorithms that exhibit higher levels of inaccuracy as regards Black women.[208] Algorithmic "fairness" is a goal, and algorithmic "bias" is a known and central problem, though both terms are subject to wildly varying definitions. The legal turn to stakeholder participation, too, reflects the bottom-up-governance principle of "nothing about us without us," originating in the disability rights movement, that motivates participatory design.[209]

At the same time, however, the reality of lawmaking is that the new law of AI and recent data protection laws still lean heavily on self-regulation by the private sector. Lawmakers aren't setting specific substantive standards—perhaps because they can't, at least not yet. They're delegating risk management to the private sector, without a lot of oversight. It's all very nice for NIST to trumpet impacted stakeholder involvement, but it's doing so as soft-law guidance without any real threat of enforcement. Stakeholder input

---

[207] Kaminski, *The Developing Law of AI*, *supra* note 24.
[208] *See e.g.*, JOY BUOLAMWINI, UNMASKING AI (2024).
[209] COSTANZA-CHOCK, DESIGN JUSTICE, *supra* note 21.

is largely permissive; companies *may* do it, but they don't have to.

We are witnessing the high-minded ideals of bottom-up governance and participatory equity shoveled into the practical framework of collaborative governance and enterprise risk management. This leaves current and proposed legal avenues for impacted stakeholder participation lacking along many dimensions tied to actual efficacy: their status as softer law, the lack of stakeholder ability to veto the use of a particular technology, a lack of attention to capacity building, and a lack of tailoring of information flows.[210] Thus this temporary alignment between neoliberal interests and calls for bottom-up governance has yielded a version of stakeholder participation targeted more towards *managing risks* rather than *opting out*.[211] There are real questions, too, of how much political will there might be for enabling more effective stakeholder participation in practice.

III. A Catalog of Legal Approaches to Stakeholder Participation

We identified the turn to stakeholder participation in Part I, and described reasons for it, both theoretical and practical, in Part II. Here in Part III, we provide original legal analysis to help readers parse the landscape, offering a catalog of stakeholder participation as it currently exists. We then in Part IV offer suggestions of how the law might be improved, both for new laws yet to be enacted, and for regulatory interpretations of laws already on the books.

The laws discussed here establish channels for participation by impacted stakeholders beyond general public participation and distinct from expert oversight. Beyond this commonality, there are many variations: A) in how such groups of stakeholders are referenced or defined; B) in whether laws envision and articulate modes of collective representation; C) in envisioned methods for consultation, if any are articulated; D) in documentation and reporting requirements; E) in whether laws address capacity building; F) and in when and at what level such participation takes

---

[210] Okidegbe, *supra* note 20; Gilman, *Beyond Window Dressing*, *supra* note 106; Margot Kaminski, Voices In, Voices In, Voices Out: Impacted Stakeholders and the Governance of AI, 71 U.C.L.A. L. REV. DISC. 176 (2024).

[211] Kaminski, *Developing Law of AI*, *supra* note 24; Okidegbe, *supra* note 20, at 1731 (calling for veto power in community governance of carceral algorithms).

place—at the micro level of the design and evaluation of individual systems or uses, or at the macro level of policymaking. We catalog a number of the more significant existing variations here, with an eye to enabling lawmakers to draw on a toolkit of approaches and identifying room for improvement.

A. Defining Stakeholders

We start with definitions. How do these laws refer to impacted stakeholders, as distinct from experts or general members of the public? We catalog at least three variations: (1) references to civil society organizations (CSOs), sometime explicitly noted as representing the interests of impacted groups; (2) references to "external parties," "impacted groups" or "impacted stakeholders;" and (3) references to marginalized groups in particular. There are also attempts to encourage companies to hire "diverse teams" of employees as stand-ins for the interests of impacted groups.

Some laws, like the EU AI Act, vaguely reference participation by "civil society organisations," which, given the context, we nonetheless think is meant to refer both to CSOs that hold policy expertise and CSOs that represent the interests of impacted groups.[212] The EU Digital Services Act (DSA), too, envisions heavy involvement by CSOs, for example in setting codes of conduct.[213] This leaves room for regulators to encourage participation by CSOs/NGOs that operate in a quasi-representative capacity, providing information about lived experiences with technologies.

Other laws, like the rules implementing the Colorado Privacy Act and draft rules implementing the California Consumer Privacy Act, refer to "external parties" generally, and "impacted groups" more specifically within the category of external parties. In the case of California, draft rules refer to "a subset of the consumers whose

---

[212] Artificial Intelligence Act, 2024 O.J. L 1689 art. 56(3) [hereinafter 'EU AI Act']. *See also* EU AI Act, recital 96 (referring to "relevant stakeholders, including the *representatives of groups of persons likely to be affected [by the AI system]*") (emphasis added).

[213] The EU Digital Services Act mandates the European Commission to facilitate the drawing up of European codes of conduct with the involvement of providers "and civil society organisations or relevant authorities to promote full and effective, equal participation, by improving access to online services that, through their initial design or subsequent adaptation, address the particular needs of persons with disabilities." Regulation on a Single Market for Digital Services [EU Digital Services Act], 2022 O.J. L 277 art. 47.

personal information the business seeks to process; or civil society organizations that represent consumers' or others' interests, including consumer advocacy organizations." [214] This frames impacted groups as consumers, aligned with the typical U.S. characterization of privacy as a consumer protection issue.

Multiple other laws also use the term "impacted groups." These references focus on the fact of impact, and do not distinguish between groups that are impacted by a technology, and particularly vulnerable or historically marginalized groups. The EU DSA for example refers to consultation of "*groups most impacted* by the risks and the measures they take" in risk assessment and mitigation.[215] The proposed federal Algorithmic Accountability Act of 2022 requires consultation of "impacted communities" by the FTC in rulemaking and consultation of "independent external stakeholders (such as representatives of and advocates for impacted groups" during impact assessments)."[216] The Council of Europe Framework Convention on AI states that risk mitigation shall "consider, where appropriate, the perspectives of relevant stakeholders, in particular persons whose rights may be impacted."[217]

Then there are laws that refer to vulnerable and marginalized communities in particular. The EU AI Act does so at least once, referencing in Recital 165 "inclusive and diverse design and development of AI systems, including attention to vulnerable persons and accessibility to persons with disability." [218] Both Washington State and Colorado have enacted laws governing state government use of facial recognition, and both laws require that a state government agency intending to use facial recognition must publish an "accountability report" that must include as part of its

---

[214] CAL. CIV. CODE § 7151(b) (West 2024).

[215] The DSA preamble requires that the preliminary assumptions of fundamental rights impact assessment are "tested with the groups most impacted by the risks and the measures they take." 2022 O.J. L 277 recital 90. In addition, recital 90 requires that VLOPs and VLOSEs "should, where appropriate, conduct their risk assessments and design their risk mitigation measures with the involvement of representatives of the recipients of the service, representatives of groups potentially impacted by their services, independent experts and civil society organisations". *Id.*

[216] Algorithmic Accountability Act, S. 3572, 117th Cong. § 3(b)(1)(G) (2022).

[217] Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, Ch. V Art. 16(2)(c).

[218] EU AI Act, recitals 81, 165.

substance a "description of any potential impacts of the facial recognition service on civil rights and liberties, including potential impacts to privacy and potential *disparate impacts on marginalized communities*."[219] Under both laws, the agency deploying facial recognition must also report on channels for receiving feedback "from *individuals affected* by the use of the facial recognition service and from the *community at large*, as well as the procedures for responding to feedback."[220] Finally, the agency under both laws must allow for public comment and hold at least three "community consultation meetings" and consider the issues raised in both comments and community meetings.[221]

The Colorado facial recognition law is one of the only laws to our knowledge to actually define the term "disproportionately impacted communities" in more detail. That definition fascinatingly suggests cross-fertilization and transplantation between environmental justice efforts and algorithmic accountability law, cross-referencing state law that established an environmental justice action task force.[222] The Colorado law defines what it means to be a "disproportionately impacted community" in reference to community cost-burden or percentage minority status (greater than 40%) and/or if the community is identified by a state agency as being subject to a "history of . . . racism."[223]

---

[219] WASH. REV. CODE §43.386.020(2)(g)-(h) (2025), https://app.leg.wa.gov/RCW/default.aspx?cite=43.386.020 (emphasis added); COLO. REV. STAT. § 24-18-302(2)(g) (2023), repeated and recodified in parts throughout the Code. *See e.g.*, COLO REV. STAT. § 24-4-109 (2024) (defining "disproportionately impacted communities").

[220] COLO. REV. STAT. § 24-18-302(2)(h).

[221] *Id*.

[222] Gilman, *Beyond Window Dressing*, *supra* note 106 (discussing Jonathan Skinner-Thompson and other materials on marginalized population participation in environmental law).

[223] COLO. REV. STAT. § 24-4-109(2)(b)(II) ("Disproportionately impacted community" means a community that is in a census block group, as determined in accordance with the most recent United States census, where the proportion of households that are low income is greater than forty percent, the proportion of households that identify as minority is greater than forty percent, or the proportion of households that are housing cost-burdened is greater than forty percent; or is any other community as identified or approved by a state agency, if: The community has a history of environmental racism perpetuated through redlining,

Several laws envision the hiring of diverse employees as an avenue for obtaining impacted stakeholder input. For our purposes here in discussing definitions of stakeholders, what is interesting is that this form of input references not just impact in general but the value of diversity in particular. For example, the NIST AI Risk Management Framework states that "[i]deally, AI actors will represent a diversity of experience, expertise, and backgrounds and comprise demographically and disciplinarily diverse teams."[224] It explains that these "[d]iverse teams contribute to more open sharing of ideas and assumptions about the purposes and functions of technology—making these implicit aspects more explicit. This broader collective perspective creates opportunities for surfacing problems and identifying existing and emergent risks."[225]

The EU AI Act, too, references the "diversity of the development teams, including gender balance" in its discussion of "inclusive and diverse design and development of AI systems."[226] This attention to diversity of development teams reflects suggestions from the design literature, which notes the ways in which homogenous developer teams can fail to catch discrimination by design. That approach, as discussed in our section on participatory design above, also faces a good deal of criticism, due both to overburdening employees and over-relying on individuals to be representative of groups and communities.

Overall, these variations in definitions of stakeholders in these laws run the gamut from referencing impacted persons in general to marginalized or diverse groups in particular. These variations reflect, we believe, differences in what regulators implicitly want

---

anti-Indigenous, anti-immigrant, anti-Hispanic, or anti- Black laws; or the community is one where multiple factors, including socioeconomic stressors, disproportionate environmental burdens, vulnerability to environmental degradation, and lack of public participation, may act cumulatively to affect health and the environment and contribute to persistent disparities. As used in this subsection (2)(b)(II), "cost-burdened" means a household that spends more than thirty percent of its income on housing, and "low income" means the median household income is less than or equal to two hundred percent of the federal poverty guideline.")

[224] NIST, AI RMF 1.0, *supra* note 89, at 9.

[225] *Id*. at 10. *See also id.* at 20, 23 ("Decision-making related to mapping, measuring, and managing AI risks throughout the lifecycle is informed by a diverse team (e.g., diversity of demographics, disciplines, experience, expertise, and backgrounds).").

[226] EU AI Act, recital 81.

these laws to do: incorporate more direct democratic participation, establish tripartism, engage in participatory design, or address and potentially remedy existing and historic harms.

B. Collective Representation

A second axis of variation is the extent to which laws envision direct participation by individual members of impacted groups, versus collective representation through representatives. Here, we focus on where laws envision a representative relationship between the stakeholders with whom the government/company engages, and a broader community or group. We also discuss whether any of the laws more precisely define what it means to represent a community or group.

A number of laws envision a representative relationship between governance participants and a community or group. Some laws are explicit about this representative role. The Colorado facial recognition law, for example, established a state task force that must by law include "one member who represents disproportionately impacted communities."[227] But many representative relationships are quietly buried in the definitions discussed above. For example, several laws rely on civil society to serve a representative role for impacted individuals and communities. Others suggest that diverse teams of employees might represent the perspectives of their communities.

Almost none of these laws squarely address what it means to "represent" a group or community. This leaves substantial room for variations in practice. Recall that in Part I, we encountered several discussions of possible modes of representation: for example, representation by geographic location versus representation by demographic group, versus mimicking the process of juror selection. [228] This vagueness also functionally delegates decisionmaking about modes of representation to government actors, private companies, and civil society organizations. Who chooses what it means to "represent" a group matters. On the other hand, attempts by the government to define representation takes agency away from communities to choose their representatives themselves.

---

[227] Colo. Rev. Stat. § 2-3-1707(1)(A)(XV) (2023).

[228] *CAB Study*, *supra* note 22 at 6; Okidegbe, *supra* note 20, at 1737-1739 (proposing a selection process analogous to jury selection).

One new form of collective representation specific to data governance is the emergence of the "data subject representative" and data cooperatives in EU law.[229] The EU recently established data stakeholders: entities envisioned as representing collective data subject rights.[230] First envisioned in the GDPR's Article 80 as a stand-in and force-multiplier for individuals in the absence of class actions in the EU, the "data subject representative" refers to not-for-profit entities with public interest objectives "active in the field of the protection of data subjects' rights and freedoms" who can be mandated by data subjects to "lodge the complaint on his or her behalf" in front of data protection authorities and to exercise procedural rights to receive compensations in courts "on his or her behalf."[231] Unfortunately, this envisioned representation is limited to procedural rights in courts or before administrative bodies, rather than substantive data governance tasks. But the concept of a data subject representative is excitingly new.

The more recently approved EU Data Governance Act (DGA) establishes the role of "data cooperatives."[232] Article 2(15) defines data cooperatives as an "organisational structure constituted by data subjects . . . having as its main objectives to support its members in the exercise of their rights with respect to certain data, including with regard to making informed choices before they consent to data processing, to exchange views on data processing purposes and conditions that would best represent the interests of its members in relation to their data, and to negotiate terms and conditions for data processing on behalf of its members before giving permission to the processing of non-personal data or before they consent to the processing of personal data."[233] Recital 31 of the DGA adds that data cooperatives might potentially find solutions to conflicting positions of individual members of a group on how data can be used, where such data relates to several data subjects within that group.[234]

---

[229] GDPR, art. 4 (defining "data subject representative").
[230] *Id.*
[231] Sylvie Delacroix & Neil D. Lawrence, *Bottom-Up Data Trusts: Disturbing the 'One Size Fits All' Approach to Data Governance*, 9 *Int'l Data Privacy L.*, 236 (2019).
[232] Data Governance Act, 2022 O.J. L. 152, art. 2(15).
[233] *Id.*
[234] *Id.*, recital 31.

C. Methods for Consultation

The laws also envision different methods of consultation: how should stakeholder input be gathered? Many just refer to consultation generally, without illustration. The GDPR's Guidelines more specifically envision the use of surveys.[235] The EU DSA, by contrast, goes beyond surveys to also reference "focus groups, round tables, and other consultation and design methods."[236] The proposed 2022 federal Algorithmic Accountability Act refers to meaningful consultation and then specifically references participatory design, which itself invokes a diverse set of practices and processes, as discussed above.[237] Other laws establish task forces (as with the Washington facial recognition law) or similar advisory fora (as with the EU AI Act).[238]

D. Capacity Building

Capacity building is a crucial, if not the crucial, component of successful external stakeholder participation.[239] These laws rarely address it, and none, to our knowledge, fund capacity building explicitly for impacted stakeholders.

Several laws do, however, discuss "AI literacy" of the public as a policy goal. The Council of Europe's Convention refers to ensuring "adequate digital literacy and digital skills for all segments of the population."[240] The EU AI Act more specifically notes that "AI

---

[235] Art. 29 Data Prot. Working Party, *DPIA*, *supra* note 14.

[236] EU Digital Services Act, recital 90.

[237] Algorithmic Accountability Act of 2022, H.R. 6580, 117th Cong. § 3(b)(1)(G) (2022) (requiring covered entities "to the extent possible, to meaningfully consult (including through participatory design, independent auditing, or soliciting or incorporating feedback) with relevant internal stakeholders… and independent external stakeholders (such as representatives of and advocates for impacted groups, civil society and advocates, and technology experts) as frequently as necessary.").

[238] EU AI Act Advisory Forum, Article 67.

[239] Kaminski & Malgieri, *Algorithmic Impact Assessments Under the GDPR, supra* note 56 at 128-129, Gilman, *Beyond Window Dressing*, *supra* note 106; Skinner-Thompson, *supra* note 101, at 467.

[240] Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, art. 20 ("Each Party shall encourage and promote adequate digital literacy and digital skills for all segments of the population, including specific expert skills for those responsible for the identification, assessment, prevention and mitigation of risks posed by artificial intelligence systems.").

literacy should equip providers, deployers and *affected persons* with the necessary notions to make informed decisions regarding AI systems."[241] The AI Act defines AI Literacy as the "skills, knowledge and understanding that allows providers, users and *affected persons*…to gain awareness about the opportunities and risks of AI and possible harm it can cause." [242] This could serve as the justification for capacity building in practice.

E. Recording and Reporting Requirements

One common feature of nearly all of these laws is that their reliance on impacted stakeholder participation is typically voluntary rather than required. The relative softness of these laws is, we believe, a consequence of their place in what is primarily a risk management framework. Regulators have repeatedly characterized impacted stakeholder involvement as a tool of risk mitigation, and delegated to regulatory entities their decisions as to what level of risk mitigation is appropriate. Most laws encourage impacted stakeholder consultation without requiring it, using permissive language such as "*may* involve,"[243] or "to the extent possible,"[244] or "where appropriate."[245]

The NIST AI Risk Management Framework used stronger, more mandatory language in an earlier draft, but the final draft is more permissive and vague about external impacted stakeholder involvement.[246] No laws, to our knowledge, require that companies or agencies must adopt stakeholder recommendations; rather, they suggest that they consult with them and consider recommendations. This gives rise, without additional regulatory oversight, to the strong possibility of participation-washing and consultation fatigue as stakeholders realize their efforts will not be taken into account.

---

[241] EU AI Act, recital 9.
[242] EU AI Act art. 3(56).
[243] Proposed CPPA Regulations, *supra* note 21, § 7151(b).
[244] Algorithmic Accountability Act of 2022, H.R. 6580, 117th Cong. § 3(b)(1)(G) (2022).
[245] EU AI Act, recital 96.
[246] For example, in the final draft, Govern 5.1 was changed from requiring integration of "external stakeholder feedback regarding the potential individual and societal impacts related to AI risks" to simply requiring "feedback from those external to the team." Likewise, in the final draft, Govern 5.2 was narrowed to require not that AI actors "regularly incorportae adjudicated stakeholder feedback into system design and implementation,"' but incorporate feedback specifically "from relevant AI actors" only. NIST, AI RMF 1.0, *supra* note 89, at 24.

Some laws creatively use recording and reporting requirements to nudge towards something more like a requirement. For example, the draft California regulations would require businesses to explain why they have not consulted external stakeholders, including impacted stakeholders, during risk assessments. [247] Another approach is to require businesses to list the stakeholders consulted in reports to regulators, a necessary precursor to meaningful regulatory oversight.[248]

F. Consultation at What Level? Micro Versus Macro Levels of Consultation

Finally, we find that laws deploying impacted stakeholder participation tend to do so at one or both of two levels: the applied level of governing individual technologies or uses through a risk assessment process, and the broader society-wide level of policy-setting.

As we saw in Part I, often these laws build impacted stakeholder participation into an impact assessment process regarding specific technologies deployed in specific settings. These laws call on the developers and/or deployers of data analytics, algorithms, and AI to consult impacted stakeholders in the identification and assessment of risks, and sometimes also in the development of risk mitigation tactics with respect to a particular technology or application of technology.

---

[247] CAL. CODE REGS. TIT 11, § 7151(b) (proposed Nov. 22, 2024). ("For the uses of automated decisionmaking technology or artificial intelligence set forth in section 7150, subsections (b)(3) and (b)(5), if the business has not consulted external parties in its preparation or review of the risk assessment, the risk assessment shall include a plain language explanation addressing why the business did not do so and which safeguards it has implemented to address risks to consumers' privacy that may arise from the lack of external party consultation.").

[248] The Algorithmic Accountability Act requires covered entities to document "any consultation with relevant stakeholders" within the impact assessment, including "any recommendations made by the stakeholders that were used to modify the development or deployment of the automated decision system … as well as any recommendations not used and the rationale for such nonuse." Algorithmic Accountability Act of 2022, H.R. 6580, 117th Cong. § 4(a)(2)(C). The Act requires covered entities to make a summary report to the FTC about the impact assessment process that must identify any stakeholders consulted and document the existence and nature of any legal agreements between the stakeholders and covered entity. *Id.* § 3(b)(1).

Other laws, however, require consultation of impacted stakeholders by policymakers setting broader policy. For example, the EU AI Act establishes an Advisory Forum to offer input to the Commission as it sets and enforces policy at a broader level, including labeling new uses as unacceptably risky.[249] A proposed 2021 Washington state bill on automated decision-making would have required state officials to consult with stakeholders "whose rights are disproportionately impacted by automated decision systems as demonstrated by current studies" when rulemaking on what constitutes "discrimination" and "less favorable treatment."[250] This would have created a special consultation track for impacted and likely marginalized groups. And the proposed 2022 federal Algorithmic Accountability Act would have required the FTC to promulgate regulations in consultation with multiple sets of specific stakeholders, including "impacted groups." [251] Similarly, the Council of Europe proposal required that countries "shall seek to ensure that important questions raised in relation to artificial intelligence systems are, as appropriate, duly considered through public discussion and multistakeholder consultation."[252]

As we discuss below, given the strong possibility of consultation fatigue, regulators should be thinking critically about how to channel impacted community participation from the as-applied level to the policy level. Rather than having to participate repeatedly in as-applied analysis, impacted groups should to the extent possible also have input into general policymaking.[253]

---

[249] EU AI Act, ch. VII art. 67.

[250] S.B. 5116, 67th Leg., Reg. Sess. § 3-4 (Wash. 2021).

[251] Algorithmic Accountability Act of 2022, H.R. 6580, 117th Cong. § 3(b)(1)(G) (2022).

[252] Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, art. 19.

[253] *See e.g.*, Sophie Toupin & Fenwick McKelvey, *Northern Lights and Silicon Dreams: AI Governance in Canada* (Apr. 2024) ("On the basis of four consultation activities happened in Canada and on the basis of their counter-consultation studies, the report recommends that new, more equitable, diverse, and inclusive forms of public participation must be identified and implemented for the ethical and human-centered development of AI to create ongoing relationships based on mutual benefit, reciprocity, equity and justice." (internal quotations omitted)).

IV. Suggestions for Improvement

We don't believe impacted stakeholder participation by itself is enough to afford adequate accountability or even to reach all the goals described in Part II. But we believe there are good reasons to have it, and that the law that structures it can be meaningfully improved.

The problem of how to enable meaningful and effective impacted stakeholder participation is bigger than the law.[254] It involves organizational design and technological practices, and significant capacity building beyond the law on the books. What we focus on here is how to better design the legal scaffolding around these things, rather than coming up with a definitive set of answers.

Our main takeaways are as follows:

First, if policymakers truly want to make impacted stakeholder participation more meaningful, they need to give it teeth. That is, they need to harden the law, which currently largely characterizes these measures as voluntary. It is not clear that there is political appetite or capacity to make stakeholder participation mandatory and require governments and companies to comply with its output, but we list several ways in which policymakers can nonetheless more meaningfully harden the law.

Second, policymakers need to get serious about capacity building, especially with the proliferation of forums in which they now expect impacted stakeholders to participate.

Third, while acknowledging our disciplinary constraints as lawyers, we offer some substantive suggestions tracking two issues identified in Part III above: how to better define "impacted stakeholders," and how to better think about designing participation modes.

Our next set of suggestions involve thinking bigger-picture

---

[254] *See e.g.*, Frank Fischer, *Participatory Governance: From Theory to Practice*, in THE OXFORD HANDBOOK OF GOVERNANCE 457, 469 (David Levi Faur ed., 2012) ("the evidence about new forms of participatory governance illustrates that participation poses difficult issues with no simple solutions."). *See also* Fernando Delgado, Stephen Yang, Michael Madaio & Qian Yang, *Stakeholder Participation in AI: Beyond 'Add Diverse Stakeholders and Stir'*, (Nov. 1, 2021) (published on arxiv.org), https://arxiv.org/abs/2111.01122 ("For AI practitioners who are interested in taking a participatory approach to AI design/development, it remains challenging to assess the extent to which a participatory tactic or process can actually achieve inclusiveness or fairness goals").

about stakeholder participation as a matter of regulatory design. Policymakers should be able to articulate why they are involving impacted stakeholders and connect their reasons to how they design for stakeholder input, with the caveat that we understand laws are enacted as a matter of political compromises and often are based on several reasons at once.

Policymakers should also focus on the overall regulatory picture. They should understand impacted stakeholder participation as one aspect of what we call "robust accountability," designing for links and interactions between it and other avenues of accountability, including expert oversight. Policymakers should increase their focus on impacted stakeholder participation at the macro/policy level, and design better ways to link micro-level participation to macro-level policy setting to avoid participation fatigue.

Finally, we call for a reframing of "impacted stakeholders" as "impacted rights-holders," reflecting our understanding that ultimately these newly developing procedural roles reflect attempts at protecting underlying rights, including substantive rights that have yet to be fully developed by courts. Policymakers should, at minimum, be thinking about group procedural rights and what those might look like and avoid foreclosing important feedback loops allowing these rights to become more substantive over time.

A. Harden the Law

If lawmakers are serious about making impacted stakeholder participation meaningful, the lowest-hanging fruit is to harden the law. This is well within policymakers' capabilities, even where an established legislative framework makes impacted stakeholder consultation merely voluntary.

Law can be harder or softer along multiple axes.[255] Hard law is mandatory and enforceable—think legislation backed by state enforcement. The hard-law version of impacted stakeholder participation would both a) require it rather than make it voluntary, and b) require governed entities to obey stakeholder input, backed by state enforcement. This is similar to what Okidegbe envisions vis-à-vis the regulation of government algorithms: stakeholder input as controlling governance, or at least as affording impacted

[255] Kenneth W. Abbott & Duncan Snidal, *Hard and Soft Law in International Governance*, 54 INT'L ORG. 421 (2000).

stakeholders an opportunity to veto certain uses of technology.[256]

But so many of these laws have been enacted characterizing impacted stakeholder involvement as voluntary risk mitigation measures. This indicates a distinct lack of political will, reflecting a tendency towards softer law and delegated self-regulation more generally speaking If we are being generous, some of the voluntary nature of these measures stems from a concern about compliance costs and the capacity of regulated entities, especially entities that raise lower risks to fundamental rights.

We nonetheless offer several ways in which regulators can harden the legal framework. In particular, we agree with Okidegbe that the law must in some way make stakeholder engagement more than merely advisory or risk considerable participation fatigue.[257] Why should impacted stakeholders repeatedly engage in impact assessment processes if they feel their feedback is not meaningfully being taken into account?

First and most obviously, policymakers could, in fact, write laws making impacted stakeholder consultation mandatory. This should be fairly feasible when they are regulating government conduct, especially at a policy-making level. For example, policymakers can require policy-setting forums to take impacted stakeholder input into account. One example of this, albeit nascent and imperfect, is the EU AI Act's requirement that technical standards-setting organizations that have been delegated significant policymaking decisions around AI systems enable and attend to impacted stakeholder participation.[258] This has resulted in an increase of participation by a wider-than-usual set of stakeholders in technological standards-setting around the AI Act at European standards organizations.[259]

It may be harder to garner the political will to make stakeholder participation mandatory when policymakers are regulating the private sector at the micro level of impact assessments for one AI system at a time, because of concerns about compliance costs and the purported need for highly contextual assessments of risk. But

---

[256] Okidegbe, *supra* note 20, at 1731.
[257] *Id.* at 1727-29. *See also CAB Study*, *supra* note 22, at 177-78.
[258] EU AI Act, recital 150.
[259] *Id.* (mentioning the European Committee for Standardization (CEN), the European Committee for Electrotechnical Standardization (CENELEC) and the European Telecommunications Standards Institute (ETSI)).

regulators could, following the example of the drafts advanced by the California Privacy Protection Agency, institute recording and reporting requirements that nudge companies towards always or at least regularly involving impacted stakeholders. More specifically, regulators could require companies to explain why they have *not* sought out the views of impacted stakeholders.

When it comes to making input meaningful, regulators could write laws establishing a hard veto for impacted stakeholders. That is, if impacted stakeholders say a company should not deploy a technology, regulators could require a company to heed this veto. Short of establishing vetoes, they could again lean on reporting requirements. Regulators could require regulated entities to flag when they choose to ignore stakeholder input—for example, to record and report when stakeholders object to a practice or design element, but they deploy it anyway.

Regulators could themselves establish formal policies for taking impacted stakeholder objections into account. For example, they could establish a threshold of stakeholder objections that would trigger intensified regulatory oversight or even bans or recalls (under the EU AI Act, for example). This would give teeth to the NIST recommendation that impacted stakeholders be allowed to collectively object to the use of an AI that has already been implemented. Regulators could encourage impacted stakeholders to bring forward evidence of repeated practices of company inattention when, for example, making arguments for labeling practices as unacceptably risky.[260]

Regulators could take part in or host stakeholder participation activities to guarantee the honesty of the process and the independence and autonomy of the stakeholders in it (though this could be risky when impacted stakeholder groups have interests counter to the government, and histories of marginalization vis-à-vis public governance). Regulators could, too, establish certain substantive backstops, such as banning systems that cannot be effectively explained to impacted stakeholders.[261]

We are aware that in some circumstances, different stakeholders might have conflicting views, making it difficult to reach a "fair" conclusion. However, stakeholder participation is not a mere "survey" of different views but a process of dialogue and a

[260] EU AI Act, ch. VII, art. 67.
[261] Okidegbe, *supra* note 20, at 1735, 1740.

methodology of joint construction of final decisions, products, solutions, and business models. Discussing different methodologies is beyond the scope of this paper and the competences of its authors, but we can refer to existing scholarship.[262]

There can be costs, to be sure, to over-hardening the law of stakeholder input.[263] It could, as mentioned, overwhelm smaller companies with compliance costs. It could over-burden or spread thin the resources of impacted groups, absent effective capacity building. It could reduce experimentation with different modes of participation, including more cooperative ones. Over-empowering impacted stakeholders could in the worst case also create an avenue for policy capture by better-resourced stakeholder groups, unintentionally disempowering more vulnerable groups.

But regulators should consider how to both harden the requirement of stakeholder consultation at least for higher-risk deployments of AI systems, and giving impacted stakeholders recommendations more force. Otherwise, impacted stakeholders will readily burn out. One possible solution would be for the laws (or regulators) to provide specific public funding for stakeholder participation. The structure and model of this funding are beyond the scope of this paper. Here we can simply refer to different potential funding frameworks or participatory activities, such as government budgets funding stakeholder associations which will participate in stakeholder consultation, raising revenue through sanctions on Big Tech, or imposing a specific tax on tech entities producing risks to fundamental rights.

B. Be Serious about Capacity Building

We turn next to capacity building. As we note above, few laws pay any attention to capacity building beyond passing references to public AI literacy.[264] The nascent critical literature already abounds with calls for capacity-building. Impacted stakeholders need to be given funding. They also need to be given adequate information and access to technological resources to be able to effectively and

---

[262] See e.g., Danish Board of Technology, *Participation Methods*, https://tekno.dk/service/participation/?lang=en (offering a catalog of participation methodologies including citizen summits, personalized presentations and courses, and scenario workshops). *See also* Vaughn & Jacquez, *supra* note 202; COSTANZA-CHOCK, DESIGN JUSTICE, *supra* note 21, at 98-99.

[263] Thanks to Federica Casarosa for this important observation.

[264] EU AI Act, art. 4 (referring to AI literacy).

meaningfully participate in governance.[265]

As we have noted here and elsewhere, so much of the new law of AI systems and data governance relies on cooperative governance with the private sector.[266] In Europe in particular, this has resulted in an unimaginable proliferation of different governance forums, both formal and informal. In terms of formal governance settings, impacted stakeholders will be chasing policy-setting at the AI Office/Advisory Forum, in European standards-setting organizations, and at the national level, through supervisory authorities that can include data protection authorities or other existing regulators. And that's just under the AI Act. Informally, policy-setting occurs every time a regulated entity undergoes an impact assessment/conformity assessment. If impacted stakeholders are to realistically participate everywhere Europe now wishes to rely on them, they must be better enabled.

Laws or guidance could consider allocating, or requiring the allocation of funding by the private sector, for impacted stakeholder participation. We are aware that in practice, there may be little political appetite given the preference for lighter-touch regulation here. [267] Participation requires energy, competence, time for preparation, education, and costs (including, e.g., for travel). Depending on the nature of the stakeholder groups invited, they might not be able to afford the time and costs for training and other participatory activities. If they are temporarily "hired" by the company that is going to develop the AI and data system, their ability to contest the system might be limited, even if they represent an external entity. This is why states might fund or co-fund stakeholder participation. Public funding might also mitigate another recurring criticism of participatory approaches, i.e., the risks that subject-matter experts could not afford the costs of a participatory design and that binding rules on stakeholder participation might be an anti-competitive barrier to entry into the

---

[265] Gilman, *Beyond Window Dressing*, *supra* note 106; Kaminski & Malgieri, *Algorithmic Impact Assessments Under the GDPR, supra* note 56.

[266] Kaminski, *Binary Governance, supra* note 54; Kaminski, *Regulating the Risks of AI, supra* note 23; Kaminski & Malgieri, *Algorithmic Impact Assessments Under the GDPR,* supra note 144.

[267] *CAB Study*, *supra* note 22, at 174 (noting boards often aren't adequately resourced). *See also* Gilman, *Beyond Window Dressing*, *supra* note 106.

market.[268]

Existing NGOs and stakeholder representative associations could contribute to a reliable and honest process. However, the issue of funding remains crucial. In some cases, these associations are funded by the group represented in the association; a clear example is trade unions. In other cases, funding might be based on alternative forms of monetization; this might be the case of data cooperatives under the EU Data Governance Act [269] or other forms of data intermediaries,[270] which might indeed find resources in part through the monetary values of personal data that their data subjects share with data controllers. [271] However, self-funding and data monetization are extremely controversial issues. That is why a clear and transparent system of public funding could be essential for the functioning of the whole stakeholder participation system.

Especially where stakeholder participation is part of private sector self-governance processes like impact assessments, regulators should also be attentive not just to which stakeholders were consulted but to *what information and resources they were provided*. New laws, or guidance for the implementation of existing laws, could codify that stakeholders must be provided access to external and neutral third-party experts. Laws could call for institutional arrangements that blend different kinds of expertise in oversight: policy expertise, technological expertise, and impacted stakeholder experience.[272]

That is, rather than envisioning expert and impacted stakeholder oversight in parallel, laws might start to consider how they could be blended together. Laws or guidance could call for stakeholder education: educating impacted individuals about the risks, [273]

---

[268] This is the reason why the European Parliament proposal of the AI Act limited the duty to consult stakeholders only to big enterprises, excluding SMEs. EU AI Act, art. 29a(4), Amendment 399.

[269] *See* Data Governance Act, 2022 O.J. L. 152, art. 2(g).

[270] See Heleen Janssen & Jatinder Singh, *The Data Intermediary*, 11 INTERNET POL'Y. REV. 1 (2022).

[271] *See e.g.*, Mydatatrust, https://www.mydata-trust.com/ (monetizing protection of life sciences data).

[272] Okidegbe, *supra* note 20, at 1734.

[273] Mireille Hildebrandt, *The Dawn of a Critical Transparency Right for the*

implications, design affordances, and disaffordances [274] of the system and about procedures for delegating meaningful representatives who could represent their needs, interests, and risks.[275]

We call, too, for regulators to pay better attention to capacity building on the company side around stakeholder engagement. Several laws call for training developers and users of AI systems on how to use AI and the risks of AI systems. [276] They could additionally call for training workers and designers about the specific communities that are involved in the stakeholder participation, their dynamic contexts, their needs and values, and their capabilities and vulnerabilities.[277] In other words, regulators should think about how designers and stakeholders could better meet halfway in a fundamental shift from transparency to critical education on the stakeholder side and from training to community-context understanding on the designer side. Costanza-Shock calls, for example, for workshops of mutual exchanges in which designers critically educate the stakeholders and stakeholders critically inform the designers about their communities, values, and contexts.[278]

C. Improve Definitions of "Impacted Stakeholders," Participation Modes

As we noted in Part III, current laws vary in how they define "impacted stakeholders," and in whether and to what extent they articulate participation modes. We here offer a few substantive suggestions, mindful of our disciplinary limitations as lawyers. The answers here are developing, unclear, and not necessarily legal in nature. But we still think it can be done better.

First, we discuss the law of who should be at the table. This is

---

Profiling Era 41, in DIGITAL ENLIGHTENMENT YEARBOOK 2012 (Jacques Bus, Malcolm Crompton, Mireille Hildebrandt, George Metakides eds., IOS Press 2012).

[274] COSTANZA-CHOCK, DESIGN JUSTICE, *supra* note 21, at 84.

[275] Todd Hartman, Hellen Kennedy, Robin, Steedman & Rianne Jones, *Public Perceptions Of Good Data Management: Findings From A UK-Based Survey*, 7 BIG DATA & SOCIETY, 1 (2020). *See also* Chih-Hsing Ho & Tyng-Ruey Changt, *Governance of Communal Data Sharing* 202, in GOOD DATA (Angela Daly, S. Kate Devitt & Monique Mann eds., 2019).

[276] EU AI Act, art. 13; S.B. 22-113, COLO. REV. STAT. 24-18-305 (2024).

[277] HRIA Toolbox, *supra* note 119, at 27.

[278] COSTANZA-CHOCK, DESIGN JUSTICE, *supra* note 21, at 91-92.

crucial: as Costanza-Chock summarizes, "if you are not on the table, you're on the menu."[279] Selecting who should be at the table—who constitutes an "impacted stakeholder"—is itself a moment of governance design and institutional selection.[280] The question is not just who constitutes an impacted group but which entities or institutions should select who constitutes an impacted group. Who are the gatekeepers? On the one hand, there are problems with delegating selection to the government. On the other hand, a broad definition by the government leaves selection largely in the hands of industry, or regulated government entity.

Lawmakers could issue or encourage the formation of guidance on best practices for selecting stakeholders—whether more formally, as codes of conduct, or informally, through agency workshops or soft-law recommendations. This brings us to a recurring theme of our recommendations in this subpart: *impacted groups should have input into regulatory guidance on impacted stakeholder participation at a policy level*. That is, as regulators formulate best practices, or as they supervise the formation of industry-led codes of conduct, they need to enable impacted groups and communities to have meaningful, even decision-making, input into those best practices. It is not enough to reference consultation of impacted stakeholders in impact assessments. Impacted stakeholders and their representatives should be involved in or even prioritized in policymaking around how such as-applied consultation might occur.

There are plenty of substantive suggestions regulators or companies could draw on when formulating best practices for selecting impacted stakeholders. For example, the European Center for Not-for-profit Law and Access Now suggest conducting a preliminary impact assessment before an actual impact assessment, in which proxies of impacted communities and high-risk groups

---

[279] *Id.* at 84.

[280] Levin, *Criminal Justice Expertise*, *supra* note 121 (noting that referring to and involving "lived expertise" then makes into a significant moment of governance the selection of who has lived expertise). *See also* Paddy Leerssen, *The Soap Box as Black Box: Regulating Transparency in Social Media Recommender Systems*, 11 EUR. J.L. & TECH. 1, 21 (2020)("[I]t is in defining and institutionalising these notionally independent groups that problems are likely to emerge").

could be initially identified.[281] They stress the importance, however, of continuing to query who is missing at the table and being open to involving more and more groups as the process goes on.

The Danish Institute of Human Rights proposes a "power map," i.e., a map where stakeholders are placed in a matrix with two axes, the first axis representing the influence of the stakeholder on the project or activities (influence/power axis), and the second representing the level of impact of the business project or activities on the stakeholder (impact axis).[282] Others suggest that the criterion for preferring some stakeholders over others should turn on the magnitude of their interests and needs at stake and the severity and likelihood of the potential impact of the data or AI system on them, also considering their vulnerabilities.[283]

In addition to mapping power, impact, and rights, it is important to pragmatically consider the *feasibility* of involving meaningful groups of stakeholders. Involvement feasibility and effectiveness depend on the existence of already established groups, associations, or entities that might represent end users in particular communities or marginalized contexts for particular needs and conditions. They might include already existing institutional representatives (e.g., trade unions), international associations (e.g., UNICEF for children, UNHCR for refugees, etc.),[284] NGOs that represent end-users (data subject associations, consumers associations, disability forums, etc.), and groups of "witnesses" of vulnerabilities (e.g., parents for children, caregivers for elderly people, etc.). In addition, these associations and entities may have experts on specific marginalizations or vulnerabilities (e.g., experts on children, on consumer cognitive vulnerabilities, etc.)[285] that could guarantee that needs and risks are assessed from objective and subjective

---

[281] European Center for Not-for-Profit Law & AccessNow, *Towards Meaningful Fundamental Rights Impact Assessments Under the DSA* 19 (2023), https://ecnl.org/sites/default/files/2023-09/Towards%20Meaningful%20FRIAs%20under%20the%20DSA_ECNL%20Access%20Now.pdf [https://perma.cc/94UZ-K28H].

[282] HRIA Toolbox, *supra* note 119, at 12.

[283] See Gianclaudio Malgieri & Cristiana Santos, *Assessing the (Severity of) Impacts on Fundamental Rights*, 56 COMPUT. L. & SEC. REV. 1 (2025).

[284] HRIA Toolbox, *supra* note 119, at 31-41.

[285] ALESSANDRO MANTELERO, BEYOND DATA: HUMAN RIGHTS, ETHICAL AND SOCIAL IMPACT ASSESSMENT IN AI (2022).

perspectives.[286] These solutions should be mindful of the limits of "deference epistemology", i.e. avoiding relying only on privileged members of impacted groups because of the elite capture of social marginalization (e.g., Brown tenured professors representing racially marginalized communities).[287] Innovative solutions could, e.g., build on recent methods proposed under the Participatory Action Research theories.[288]

Regulators could do a better job, too, of articulating how input should occur. The GDPR guidelines' reference to surveys, for example, is wholly disappointing and inadequate, rendering stakeholder participation a formality. There are extensive resources now available on institutional design for stakeholder participation in particular. Regulators should reference and consider these, including by incorporating them into guidance. We offer just a few examples here.

The Danish Institute for Human Rights explains that during impact assessments, there are typically two kinds of participation procedures: (1) the collection of information about impacts, needs, and expectations of stakeholders in the design and use of certain systems, and (2) participatory decisions about how to design, develop, and/or employ a specific system. The collection of information is essential in participatory impact assessments.[289] Collecting information might happen in intermediated ways (e.g., surveys, interviews) or via workshops. The second element, participatory decisions, could follow specific procedures, e.g., based on majority rules, unanimity, or consensus.[290]

Gilman draws on examples of more or less successful structuring of public participation in other areas of the law:

---

[286] HARRY COLLINS, ROBERT EVANS, DARRIN DURANT & MARTIN WEINEL, EXPERTS AND THE WILL OF THE PEOPLE: SOCIETY POPULISM AND SCIENCE (2020).

[287] *See* Olúfẹ́mi Táíwò, *Being-in-the-Room Privilege: Elite Capture and Epistemic Deference*, 108 THE PHILOSOPHER 61 (2020) (laying out the 'elite capture' criticism).

[288] See, e g., Cornish, *supra* note 165, at 34. For an overview of different participatory methods, see Vaughn & Jacquez, *supra* note 202.

[289] *See generally* HRIA Toolbox, *supra* note 119.

[290] *See e.g.*, Danish Board of Technology, *Participation Methods*, https://tekno.dk/service/participation/?lang=en (offering a catalog of participation methodologies including citizen summits, personalized presentations and courses, and scenario workshops). *See also* Vaughn & Jacquez, *supra* note 202.

environmental protection, poverty policy, and land use.[291] She points to extensive guidance on best practices for environmental justice efforts. This guidance includes practical recommendations on outreach and publicity to affected communities; on how to attend to logistical barriers to participation; and on a range of different participatory mechanisms (from focus groups to computer-assisted processes) and consensus-building processes.[292]

Research on participatory governance also assesses different input mechanisms beyond just surveys, including, for example, televoting, focus groups, scenario workshops, and citizens' assemblies.[293] Current law typically leaves room for a variety of approaches, but it does not channel companies or policymakers towards more effective ones. Regulators could create guidance building on existing research, with the input of impacted stakeholder groups.

As another example of how to think about designing for stakeholder input, Okidegbe writes about how to improve the design of commissions intended to enable community governance of state use of algorithms. She draws on work by K. Sabeel Rahman and Jocelyn Simonson on how to better effectuate community control.[294] Okidegbe calls, among other things, for making community stakeholder input controlling rather than advisory;[295] for affording the opportunity to veto or opt out of the use of a technology entirely;[296] for thinking seriously about how to select representative community members through a jury-pool-like process;[297] and for enabling participation in policymaking by community members and their representatives who are not serving on a particular task force or commission.[298]

---

[291] Gilman, *Beyond Window Dressing*, *supra* note 106, at 534-44.
[292] Gilman, *Beyond Window Dressing*, *supra* note 106, at 541. See Nat'l Env't Just. Advisory Council, *Model Guidelines For Public Participation: An Update To The 1996 Nejac Model Plan For Public Participation* (2013), https://www.epa.gov/sites/default/files/2015-02/documents/recommendations-model-guide-pp-2013.pdf.
[293] Fischer, *supra* note 254, at 465.
[294] Okidegbe, *supra* note 20 (discussing K. Sabeel Rahman & Jocelyn Simonson, *The Institutional Design of Community Control*, 108 CALIF. L. REV. 679 (2020)).
[295] *Id*. at 1735.
[296] *Id*. at 1734 ("This would mean that algorithmic use could be prevented through the Commission.").
[297] *Id*. at 1738.
[298] *Id*. at 1735.

Regulators also need to think more seriously about stakeholder input and timing. Most laws, as discussed, appear to largely think about stakeholder involvement as participatory design, i.e., in embedding values into technologies or in identifying risks so they can be mitigated during initial system design before systems are deployed.

Stakeholder involvement should not be a mere ex-ante exercise, happening at the design or pre-deployment stage and never after. But participation should also not be an ex-post check when AI models or data systems have already been designed or implemented in specific sectors and real changes and mitigations are not possible.[299] Ideally, stakeholder involvement would be an ongoing exercise, as part of a continuous cycle of design and impact assessment that leads to re-design and to new impact assessments,.[300] For example, the NIST Framework describes how "[i]ncreasing the breadth and diversity of stakeholder input throughout the AI lifecycle can enhance opportunities for identifying AI system benefits and positive impacts, and increase the likelihood that risks arising in social contexts are managed appropriately."[301]

Thinking about stakeholder involvement across the entire lifecycle, including deployment, will come at a cost, both in spreading stakeholders thin and imposing costs on companies. But regulators should think about how to use stakeholder involvement more judiciously. Stakeholders might, for example, play a role in the "participatory monitoring" of technological systems that are already deployed.[302] They could alert regulators to problems with systems already in use.

D. Connect Reasons to Policy Design

We now turn from our more pragmatic suggestions to the bigger picture of regulatory design.

To craft effective stakeholder participation, one must first articulate the reasons for having it.[303] This will be a challenging task

---

[299] Gilman, *Beyond Window Dressing*, *supra* note 106, at 543.
[300] *See* ECNL, *supra* note 281.
[301] NIST, AI Risk Management Framework: Second Draft 11 (Aug. 18, 2022), https://www.nist.gov/system/files/documents/2022/08/18/AI_RMF_2nd_draft.pdf.
[302] HRIA Toolbox, *supra* note 119, at 3.
[303] Kaminski, *Understanding Transparency*, *supra* note 25.

given the divergence in reasons and motivations for establishing stakeholder participation discussed in Part II. Those reasons, as we outlined, vary from trying to codify best practices from participatory design,[304] to trying to redistribute general democratic power, to trying to mitigate the historic and present underrepresentation of groups of users in situations of vulnerability, marginalization, and subordination.[305]

Different reasons lead to different interventions and impact the contours of a law. They impact, for example, how one defines who gets to participate through these channels (impacted stakeholders generally, or marginalized stakeholders in particular), and at what level the channels are placed (design of a particular technology, or broader policymaking).

While we recognize that lawmaking reflects political compromise, and that a single law can be justified by multiple reasons, it is hard to impossible to craft an effective regulatory system if we can't decide why we are creating it. Fundamentally, institutional design depends on your goals. Lawmakers should ask themselves: are they looking at stakeholder participation through the lens of deliberative democratic theory, believing in participation as a public good that improves output through consensus-building?[306] Or are they trying to structure disagreement (the agonistic approach)? Are they attempting to implement participatory design through the law, and/or make up for historic and ongoing participation inequities?

E. Conceptualize Impacted Stakeholder Participation as an Aspect of Robust Accountability

It is crucial that impacted stakeholder participation is not conceived as a standalone activity but is instead envisaged as an element of a broader system of *robust accountability*. Robust accountability means a system of accountability involving regulators, individuals, groups, and other external actors, the elements of which augment and reinforce each other's efficacy. Its inverse is ineffective accountability, where the elements hamper each other rather than augment. Accountability should be resilient:

---

[304] Young et al., *supra* note 178.
[305] MALGIERI, *supra* note 123.
[306] *See e.g.*, Fischer, *supra* note 254.

if one part falls through, other parts should be able to pick up the baton.

Impacted stakeholder governance of data and AI is a necessary but not sufficient element of robust accountability. It cannot replace all other principles and elements of accountability. We observe, instead, that participatory governance is an essential complementary element that can valorize other existing principles and elements by strengthening and reinforcing the whole cycle of accountability.

Impacted stakeholder participation in an ideal state both feeds into and benefits from expert audits, regulatory oversight, and individual rights. Connecting participatory governance to other accountability elements, including external audits, public scrutiny, design standardization, and whistleblower protections, might overcome some of the main limitations of participatory governance alone.

It is also possible, however, for other forms of accountability to be designed in ways that hamper stakeholder accountability. The creation of transparency to technological experts under constraints of nondisclosure, for example, valorizes technological expertise and oversight at the expense of impacted stakeholder information and input. A general lack of regulatory inspection and enforcement, too, would hamper even the most stringent stakeholder participation requirements. For one aspect of accountability to be effective, other aspects must work as well. And they must be designed to feed into, inform, and amplify each other.

One of us has called for regulatory attention to disclosures to stakeholders in particular.[307] Privacy laws and algorithmic accountability laws establish numerous information flows: to individuals, to the public, to experts.[308] They do not, however, typically establish information flows targeted to impacted stakeholders as groups.

Given the amount of recent attention in privacy laws to how privacy disclosures are made in other contexts, regulators could apply what they know of "effective transparency" or "meaningful

---

[307] Kaminski, *Voices in, Voices Out*, *supra* note 105. See also Gilman, *Beyond Window Dressing*, *supra* note 106, at 542.

[308] Kaminski, *Understanding Transparency*, *supra* note 25.

transparency" here.[309] They could, at the very least, require that regulators have oversight over what information companies are providing to stakeholders and how they are framing it.[310] Although we emphasize the importance of transparency, there can be a trade-off between the comprehensibility of existing design options and the specificity and granularity of what is disclosed to stakeholders.[311]

Regulators could also play a role in establishing information flows from the results of risk assessment processes to stakeholder groups or representatives. Often, risk assessments are not made public. Regulators are envisioned as the only entities with access to risk assessments in their entirety. Some laws envision a more truncated version being publicly disclosed, due to largely overblown concerns about trade secrets. Regulators could, without revealing trade secrets, close the informational gaps. For example, California's draft regulations on automated decision-making require disclosure to regulators of "[t]he results of the business's evaluations. For example, the business may provide an explanation of the performance and error metrics across demographic subgroups as part of the results of its fairness evaluation."[312] Lawmakers could either mandate that such information be made public or could establish information flows directly from supervising regulators to impacted stakeholder groups and their representatives.

F. Focus More on Macro-Level Policy-Setting and on Better Linking Micro-level Participation to Macro-Level Policy

Regulators should be more attentive to both a) increasing and amplifying impacted stakeholder participation in policy-setting at the macro level, and b) to structuring interactions between the micro-versus-macro levels of governance discussed in Part III above.

It is crucial to involve impacted stakeholders at the

---

[309] See, e.g., GDPR, art. 13-14 (providing guidelines on privacy disclosures and transparency). See also Age-Appropriate Design Code Act, A.B. 2273, Reg. Sess. (Cal. 2022) (on how to effectively communicate with children online).

[310] See, e.g., Okidegbe, *supra* note 20, at 1727 (discussing how the State is not a neutral provider of information/expertise, and how transparency from a state can construct reality. Even more true of private sector "transparency").

[311] *Id.* (criticizing transparency as non-neutral but part of epistemics/knowledge production). See also Fischer, supra note 254; Kaminski, *Understanding Transparency*, *supra* note 25.

[312] Proposed CPPA Regulations, *supra* note 21, at § 7153(a)(2)(F).

policymaking level. Impact assessments are often touted as a form of early-stage experimentalist governance, implemented when policymakers know a particular technology is risky, but don't yet have evidence of how to best govern its uses.[313] They can serve an information-forcing function, and cumulatively can help regulators identify recurring risks and harms. Taking data governance law's reliance on impact assessments at face value, then, suggests that there will eventually be more substantive policy. If impacted stakeholders serve the functions at the micro-level of identifying risks and harms and holding governed entities accountable to their needs, they certainly serve the same functions at the macro-level, too. It thus makes little sense to continually point regulated companies to engaging with impacted stakeholders each time they design and deploy a technology, and not to require regulators to do the same when setting substantive society-wide policies. And as discussed above, the political hurdles to requiring regulators to consult with impacted stakeholders during policy setting are likely lower than those to requiring regulated companies to do the same. At least, there are fewer concerns regarding over-burdening regulated entities with compliance requirements.

Whatever the benefits of participatory design—and there are many—we are concerned as a matter of regulatory design with the possibility that impacted stakeholder participation will be relegated primarily to the micro-level, with impacted stakeholders involved only in the design or oversight of individual AI systems (as-applied engagement).

Under both the EU AI Act and the Colorado AI Act, there is a risk that impacted stakeholder participation will be framed solely as a risk mitigation measure that companies voluntarily partake in during the design and deployment of individual systems. While in some ways vastly different, both laws rely on compliance with "technical" standards as a safe harbor of sorts from enforcement. This potentially forecloses an important feedback loop between enforcement and substantive future policy-setting. We illustrate this as follows.

Say, for example, a company complies with NIST's suggestion that it consult with impacted stakeholders during its risk

---

[313] *See, e.g.*, Selbst, *An Institutional View of Algorithmic Impact Assessments*, *supra* note 135.

assessments, per the Colorado AI Act.[314] During said risk assessment and mitigation, a particular community objects to the use or particular design features of an AI system. But the NIST AI RMF Framework indicates that stakeholder engagement is voluntary, not mandatory. And compliance with the Framework under the Act serves as an affirmative defense to enforcement by the attorney general. Thus, the community's objection may never be disclosed to the public or to lawmakers; even the AG may never engage with it so long as the company is understood to be compliant with the AI RMF. The legal framework thus forecloses a potential feedback loop from stakeholder participation into general policy evolution.

The AI Act establishes a similar closed loop: eventually, compliance with technical standards set by European standards-setting organizations in response to a request from the Commission will serve as a sort of safe harbor from enforcement (a "presumption of conformity"). Thus, the more procedural and voluntary the technical standards, the easier it is for companies to tick boxes and be in compliance, the less likely stakeholder participation at the micro-level will be looped into a history of enforcement that then informs substantive policy development going forward.

Moreover, excluding affected communities from engagement with technology design prevents the development of expertise with that technology that could otherwise inform substantive regulation going forward.

There is also the issue of participation fatigue. To avoid participation fatigue, lawmakers should think about various kinds of force multipliers: through representation, through collectives, through connecting as-applied input to policy-level input. Lawmakers should pay more attention to how impact-assessment-level engagement could and should be connected to general society-wide policymaking. That is, despite the appeal of participatory design, lawmakers should think about ways in which micro-level input can feed into, inform, or even become policy.

G. Reframe: "Impacted Stakeholders" as "Impacted Rights-Holders"

Finally, we call for a reframing of "impacted stakeholders" as "rights-holders," drawing on literature on Human Rights Impact Assessments (HRIAs). And we call for the recognition of related

[314] Colorado AI Act, SB 24-205 (2024), § 6-1-170(2)(a)(I)(A).

group procedural rights: for example, a group right to contest AI systems, to trigger re-assessment of risks, or even spur recalls of a system.

On a fundamental level, we call for a reframing of impacted stakeholder participation as the collective participation rights of groups of individual rights-holders. Impacted stakeholders aren't just another set of stakeholders in a multistakeholder process. They are often the holders of fundamental human rights impacted by the use of these systems.[315] The fundamental right at issue may be the right to privacy, but also the right to non-discrimination and self-determination online. Although in different legal systems, there might be different qualification of these rights (e.g. while in the EU the fundamental right to privacy is mentioned in the EU Charter of Fundamental Rights and in the European Convention on Human Rights, in the U.S. Constitution there is no individual constitutional right to privacy against private actors), the international charters of human rights[316] have increasingly recognized the human rights nature of privacy.[317]

Human rights somehow get lost in all of this. This is despite the fact that DPIAs, Fundamental Rights Impact Assessments (FRIAs), and Algorithmic or AI Impact Assessments (AIAs) can trace their legacy at least in part to the HRIAs conducted under international law.[318]

As explained above, under the AI Act, FRIAs require (among many other things) a description of the "specific risks of harm likely to impact the categories of persons or group of persons" who are "likely to be affected by its use in the specific context."[319] Within this framework, the deployers of high-risk AI systems are encouraged to "involve relevant stakeholders, including the representatives of groups of persons likely to be affected by the AI

---

[315] HRIA Toolbox, *supra* note 119.

[316] *See* United Nations GAOR, The Right to Privacy in the Digital Age, 75/176 (2020). *See also* Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, European Treaty Series No. 108, https://rm.coe.int/1680078b37.

[317] See e.g., Oliver Diggelmann & Maria Nicole Cleis, *How the Right to Privacy Became a Human Right*, 14 HUM. RTS. L. REV. 441 (2014); Manuel José Cepeda Espinosa, *Privacy*, in THE OXFORD HANDBOOK OF COMPARATIVE CONSTITUTIONAL LAW (Michel Rosenfeld & András Sajó eds., 2012).

[318] MANTELERO, supra note 285, at 13.

[319] EU AI Act, art. 27.

system, independent experts, and civil society organizations in conducting such impact assessments and designing measures to be taken in the case of materialization of the risks."[320]

International human rights law itself provides rights to public participation.[321] Even where rights-holders do not have an explicit group right to participate, they typically have other intrinsically connected individual rights under data privacy and algorithmic accountability laws (e.g., a right to contest or object, a right to a new decision, a right to access and receive explanations, etc.). They have other rights, too, that range from procedural to far more substantive, including the fundamental rights of free expression, privacy and data protection, non-discrimination, and more. Accordingly, a good participatory model should not simply refer to users as "stakeholders" but as "*rights-holders*."[322]

A "lived expertise" framing may be appealing as an attempt to elevate impacted stakeholders to the same level of importance as expert oversight or policy experts.[323] But it fails to recognize the ways in which impacted rights-holders' rights should be prioritized *above* technological expertise. Invoking rights triggers the support of other institutions of governance: human rights courts, for example, and international human rights law. One of us has critiqued the ill-fit between the use of risk regulation to govern AI and the type of risks to fundamental rights and to fairness it attempts to address. If risk regulation of fundamental rights is to be made at all meaningful, groups of individual rights-holders and supporting rights-constituting institutions must be involved and prioritized. And, as noted just above, regulators must be sure not to close off important feedback loops between the formation of substantive rights through enforcement and litigation, and the largely procedural risk regulation increasingly established through standards-setting organizations.

We call attention to related principles for Indigenous Data Sovereignty as one example of a strong form of calls for collective rights over data. Indigenous Data Sovereignty "reinforces the rights to engage in decision-making [over data governance] in accordance

---

[320] EU AI Act, recital 96.
[321] HRIA Toolbox, *supra* note 119.
[322] *Id*. at 5.
[323] Okidegbe, *supra* note 20; Ngozi Okidegbe, *The Democratizing Potential of Algorithms?,* 53 CONN. L. REV. 739, 764 (2022); *but see* Levin, *supra* note 121.

with Indigenous values and collective interests."[324] The CARE Principles for data governance are grounded in internationally recognized Indigenous rights to free, prior, and informed consent in the collection and use of data.[325] The CARE Principles call, among other things, for "the right to develop cultural governance protocols for Indigenous data and be active leaders in the stewardship of, and access to, Indigenous data."[326] The Principles explain that the assessment of ethical harms and benefits "should be done from the perspective of the Indigenous Peoples, nations, or communities to whom the data relate."[327] And they demand that such processes "must include representation from relevant Indigenous communities."

We close with several concrete implications of this shift in framing. Regulators should think creatively about the ways that impacted rights-holder groups might invoke existing individual procedural rights as a collective and make these processes more effective. For example, regulators could link large-scale invocations of individual rights to contest or opt out of a decision-making system to policy-level governance of the system. That is, they could link a group right to opt out of use of such systems, to policy decisions to ban or regulate them.

Let's say a large percentage of affected individuals invoke their right to contest a particular deployed AI system. Regulators could require that a certain threshold level of contestation triggers a new risk assessment process, including new and more effective risk mitigation tactics, including system re-design, and mandatory notification of regulators. A particularly high level of contestation could even result in regulators recalling or decommissioning the system.[328] But a lack of contestation should not signify that a system

---

[324] Research Data Alliance International Indigenous Data Sovereignty Interest Group, *CARE Principles for Indigenous Data Governance* 1 (Sept. 2019), https://www.rd-alliance.org/wp-content/uploads/2024/04/CARE20Principles20for20Indigenous20Data20Governance_OnePagers_FINAL20Sept2006202019.pdf.

[325] *Id*. at 3.

[326] *Id.* at 1.

[327] *Id*. at 5.

[328] *See* EU AI Act, art. 20(1) (concerning AI deployers who can spontaneously recall AI systems that they suspect not being in the conformity with the AI Act rules). *See also* EU AI Act, art. 79(2) (on the power of market surveillance authority to require the recall of AI systems).

is okay, for all the reasons we discuss above, related to the flaws of a consent-based regime due to existing vulnerabilities and power imbalances.

Regulators could establish new pathways and information flows, from stakeholder feedback after deployment straight back into system evaluation and re-design. For example, the NIST Framework suggests establishing "[f]eedback processes for end users and *impacted communities* to report problems" and integrating this feedback and reports of contestation "into AI system evaluation metrics." [329] This is a community-driven group version of the GDPR's individual "right to express one's view.". We think in theory there is a compelling justification for a group-level right to express one's collective views, as well.

And that feedback should be incorporated into decisionmaking. The NIST Framework elsewhere suggests establishing "mechanisms… to regularly incorporate adjudicated feedback from relevant AI actors [formerly, "adjudicated stakeholder feedback"] into system design and implementation."[330]

We close by calling for drafters of new laws to consider establishing new group rights with bite. For example, many AI laws establish individual rights to opt out or contest significant AI decisions.[331] One could readily envision a group "right to contest" AI decisions. In fact, the NIST framework quietly does. Alongside the feedback process discussed above, the Framework calls for "processes for … *impacted communities* to … *appeal system outcomes*"."[332] This group's right to contest could be grounded in showing that a system is discriminatory or otherwise harmful towards a particular neighborhood, community, or group.

There could be a role for data collectives, data cooperatives or data subject representatives like those discussed above. One representative challenge could trigger a re-do of decisions for an entire segment or group. Or a group's "right to contest" could trigger a regulatory review, or even AI system recalls.[333]

Our call for reframing of "impacted stakeholders" as "impacted

---

[329] NIST, AI RMF 1.0, *supra* note 89, at 31 (measure 3.3).
[330] *Id.* at 24 (Govern 5.2).
[331] Margot E. Kaminski & Jennifer M. Urban, *The Right to Contest AI*, 121 COLUM. L. REV. 1957 (2021).
[332] NIST, AI RMF 1.0, *supra* note 89, at 31 (measure 3.3).
[333] *See* EU AI Act, art. 79(2).

rights-holders" reflects our understanding that ultimately these newly developing procedural roles reflect attempts at protecting underlying rights, including substantive rights that have yet to be fully developed by courts. Policymakers should, at minimum, be thinking about group procedural rights and what those might look like, and avoid foreclosing important feedback loops allowing these rights to become more substantive over time.

Conclusion

This Article has examined recent proposals governing AI systems and data-driven systems that have turned towards involving impacted stakeholders in the design and governance of data-driven systems that affect them. This includes impacted stakeholders in situations of contextual vulnerability or historically marginalized communities. We surveyed reasons for and a wide array of practices and policy proposals regarding impacted stakeholder participation to arrive at a catalog of possible interventions.

We acknowledge the inherent limits of stakeholder participation. That is why we proposed participatory frameworks as an essential element of a broader concept of robust accountability, envisioned as consisting of complementing requirements of substantive and procedural fairness of AI systems, critical transparency, individual rights, and external audits.

We closed with a call for re-framing impacted stakeholders as collective rights-holders and for the recognition of several variations on group rights, including a group right to express a view and to contest AI. Several laws, most notably the GDPR, already afford individual rights to "express one's view" and to contest AI systems. Impacted rights-holders should be empowered to collectively leverage and invoke the kinds of rights individuals are already afforded.