6-2021

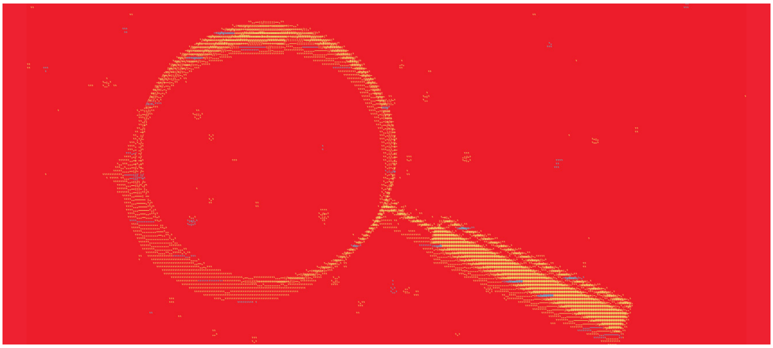
Transparency's AI Problem

Hannah Bloch-Wehba
Texas A&M University School of Law, hbw@law.tamu.edu

Recommended Citation

Hannah Bloch-Wehba, *Transparency's AI Problem*, (2021).
Available at: https://scholarship.law.tamu.edu/facscholar/1477

DATA AND DEMOCRACY



Transparency's AI Problem

By Hannah Bloch-Wehba

KNIGHT
FIRST AMENDMENT
INSTITUTE at
COLUMBIA UNIVERSITY

In October 2020, the Knight First Amendment Institute at Columbia University convened a virtual symposium, titled “Data and Democracy,” to investigate how technological advances relating to the collection, analysis, and manipulation of data are affecting democratic processes, and how the law must adapt to ensure the conditions for self-government. This symposium was organized by the Institute’s 2019-2020 Senior Visiting Research Scholar, Yale Law Professor Amy Kapczynski, and co-sponsored by the Law and Political Economy Project at Yale Law School.

The essays in this series were originally presented and discussed at this two-day event. Written by scholars and experts in law, computer science, information studies, political science, and other disciplines, the essays focus on three areas that are both central to democratic governance and directly affected by advancing technologies and ever-increasing data collection: 1) public opinion formation and access to information; 2) the formation and exercise of public power; and 3) the political economy of data.

The symposium was conceptualized by Knight Institute staff, including Jameel Jaffer, Executive Director; Katy Glenn Bass, Research Director; Amy Kapczynski, Senior Visiting Research Scholar; Alex Abdo, Litigation Director; and Larry Siems, Chief of Staff. The essay series was edited by Glenn Bass with additional support from Lorraine Kenny, Communications Director; A. Adam Glenn, Writer/Editor; and Madeline Wood, Communications and Research Coordinator.

The full series is available at knightcolumbia.org/research/

INTRODUCTION

ARTIFICIAL INTELLIGENCE has a serious transparency problem. AI is transforming governance, but its outcomes are difficult to explain, and its processes impossible for lay users to understand.[1] What's more, the AI tools governments increasingly rely upon to automate decision making are often procured from private sector vendors, compounding the public's inability to ascertain what it is, exactly, that government is doing when it uses AI. Together, these two features have led scholars to critically assess the transparency and accountability of AI tools and techniques, and to try to improve AI's design and performance to satisfy these essential values.[2]

Yet there is little consensus on what algorithmic transparency actually means. In a technical sense, experts have described AI's machinations and determinations as "opaque" because they are difficult to explain or to articulate, even to experts.[3] But even systems that are technically transparent can remain opaque in a legal and political sense. Automated decision systems are often procured in secret or with limited public oversight. Open-government obligations like the Freedom of Information Act and state public records laws do not directly reach the private sector vendors that supply AI/ML technology to the government. Today, private companies hold a near-monopoly on critical information about the ethical, legal, political, and technological ramifications of AI, with few concomitant responsibilities to release it to the public.[4]

Government and public institutions' use of automation thus fosters opacity on two basic levels: the technical and the political-economic. At least in theory, innovation can address—to a greater or lesser extent—technical barriers to transparency.[5] But the central role that law affords the private sector in developing and implementing AI in government bears equal responsibility for opacity as does technical sophistication.

Insulating private vendors from scrutiny produces negative consequences for democracy. We need to know what automated decision systems governments are using, how they work, and what their effects on individuals and society are. Without some baseline level of public-facing transparency, democratic principles of control and participation become elusive. But at precisely the same moment at which calls for algorithmic transparency and accountability are reaching a fever pitch, we have contracted out substantial portions of public governance to a virtually unregulated industry that operates largely in the shadows. This industry itself wields substantial influence in crafting arguments about the rightful scope and extent of transparency obligations, and the gaming, secrecy, and commercial interests on the other side of the balance.

This essay begins to sketch an agenda for rendering this private control transparent and accountable to the public. I argue for direct and meaningful algorithmic transparency obligations to be imposed upon private vendors that supply AI tools to government actors. I highlight the importance of grounding those obligations in principles of direct participation and community control in governance, rather than in elite and technocratic modes of oversight.[6] In so doing, the essay adds to a body of work that considers how technology companies function as participants in our governance arrangements.[7] It also contributes to a long-standing conversation about whether and how to extend public law obligations to private actors.[8]

After briefly outlining the conceptual underpinnings of the freedom of information regime and its theoretical relationship to democratic participation and accountability, Part I maps out current approaches to algorithmic transparency in government. I show that, in the context of government's use of algorithms, open government falls short of its goals to promote information-sharing or good governance. Partly in response to these shortcomings, efforts to promote transparency in AI have shifted from a focus on disclosing the source code and data for AI tools to a focus on broader concepts of accountability and the right to an explanation. Core concepts of "accountability" and "transparency" familiar from open-government contexts are being contested, reimagined, and redefined. These methods of promoting algorithmic transparency—while essential—are not substitutes for transparency law itself, because they fail to extend the participatory democratic values that animated the Freedom of Information Act (FOIA).

Part II examines how the high stakes of automated decision making in criminal law enforcement—and the increasingly urgent calls for direct democratic participation—illustrate the limits of a technocratic approach to algorithmic accountability and transparency. When lives are on the line, demands that the affected individuals and communities should be given a meaningful voice in policy increase. In these contexts, assurances of fairness, accountability, and justice from private sector vendors are widespread, but simply not sufficient to persuade the public or assuage concerns. In response, new ex ante modes of accountability are emerging to guard against abuses and to bolster community participation and input.

Part III concludes with three proposals for how states and governments could enhance algorithmic transparency. In particular, governments can extend public values to private vendors through contracting and procurement reform. These proposals would allow government agencies to consider vendors' commitments to openness in the contracting process, alongside the dollar figure of their bids. They would also allow government agencies to begin a more aggressive push toward openness in automated decision making by conditioning contracts on data-sharing obligations. While these approaches have several drawbacks, their benefits include a fidelity to the presumption of democratic participation and democratization of data that underlies the open-government framework.

I. TRANSPARENCY AND ACCOUNTABILITY IN A CHANGING WORLD

Transparency law's democratic roots

Transparency has long been an integral aspect of administrative accountability. When Congress enacted the Freedom of Information Act in 1966, it intended to "pierce the veil of administrative secrecy and to open agency action to the light of public scrutiny."[9] FOIA was a direct legislative response to an administrative state that had become increasingly shadowy.[10] While FOIA has come to occupy a central role in scholarly thinking about transparency law, all 50 states have also enacted their own public records statutes, many of which are patterned after FOIA.[11]

In brief, FOIA and its state equivalents impose a general rule that government records ought to be open to the public.[12] Instead of designating certain categories of records as public, FOIA exhibited a presumption of disclosure upon request, subject to certain exemptions that were to be construed narrowly.[13] Those exemptions include carve outs for properly classified information, records subject to statutory secrecy requirements, trade secrets, privileged information, personnel and medical files, and records compiled for law enforcement purposes.[14]

FOIA differed from other transparency obligations imposed by the regulatory state—its transparency mandate was oriented toward the public. While a wide variety of regulatory frameworks require private industry to disclose information to regulators, FOIA requires the government to disclose information to anyone who asks. As Margaret Kwoka has shown, FOIA was "designed by journalists, for journalists," in keeping with theories of democracy that placed the press at the center of democratic self-governance.[15] Other disclosure obligations operate quite differently. Regulatory monitors, for instance, can compel firms to disclose information to government agencies, even apart from any specific investigation of a firm.[16] These disclosure arrangements are essential to the promotion of effective administrative oversight and expert regulation. But unlike FOIA, these other disclosure arrangements were never intended to promote effective public participation in democratic governance.

In several ways, FOIA and its state equivalents fall short of the goals of promoting democratic self-governance and government accountability.

First, FOIA left private industry largely beyond the reach of its disclosure obligations—and private power thus mostly undisturbed.[17] The statute's inadequate ability to reach private enterprise has dismayed observers at least since the early 2000s, particularly in the context of increasingly privatized military and security functions.[18] Amid widespread contracting-out by government, the divergence between the extensive transparency obligations borne by government agencies and the minimal ones incurred by private enterprise has resulted in a growing blind spot that at times undermines FOIA's chief objectives.[19] A large body of literature has raised significant questions about how privatization might deleteriously affect public values such as accountability and transparency.[20] The most direct and obvious transparency obstacle is imposed by FOIA's failure to reach much important information that is either shared by or remains in the hands of the private sector. For instance, in 2003, when seven crew members aboard the space shuttle Columbia died as their vessel disintegrated upon re-entering the atmosphere, NASA fielded dozens of FOIA requests related to the disaster.[21] But the records held by United Space Alliance—a joint enterprise of Boeing and Lockheed Martin that was the contractor with major responsibility for the shuttle—were off-limits because they were in the hands of a private contractor.[22]

Second, and relatedly, critics of FOIA and of the "open government" movement more generally have also observed that the statute's presumption of radical openness might exacerbate antagonism between the public and government institutions, inculcating suspicion and undermining trust. By exposing governmental wrongdoing to public scrutiny, FOIA's structure systematically contributes to a "mounting adversarialism" between government and citizens.[23]

To some degree, adversarialism can be a positive. Some amount is to be expected when many constituencies come to the policymaking table; indeed, adversarialism might be a critical aspect of "democratic contestation and control."[24] Yet to the extent that transparency mechanisms reveal and contribute to the publicity surrounding government wrongdoing, they also focus attention and distrust on government rather than on private actors who are systematically insulated from public view, amplifying the sense that government alone *deserves* that level of scrutiny and distrust.[25]

Finally, FOIA's demands themselves are exceptionally burdensome, and the benefits of open government are unevenly distributed. Instead of restricting disclosure of government information to those who had "good cause" to want it, FOIA required disclosure to "any person" who requested the records.[26] FOIA's "entitlement" to public information has led critics to argue that its benefits are systemically "rationed" through the litigation process—a process that, itself, favors wealthy private actors.[27] While FOIA's policy of disclosure to "any person" has historically been justified on the grounds that it facilitates democratic participation in government, today commercial enterprise represents an "overwhelming majority" of FOIA requests, calling this justification into doubt.[28] At the state and local level, these dynamics are even more pronounced.[29]

Algorithmic transparency and accountability

Despite these flaws, public records laws have seemed a potentially fruitful mechanism for gathering information about government institutions' uses of automation and AI.[30] On one level, using public records laws to obtain access to the instruments of algorithmic governance is appealingly straightforward: Access to source code is often necessary to understand how an algorithm works, and source code can be accessible in written form as a record subject to disclosure. And in at least one recent case, public interest litigants have succeeded in using FOIA as a mechanism to gain access to a government algorithm, a computer model that the Environmental Protection Agency used to set policy regarding greenhouse gas emissions.[31]

In other ways, however, public records statutes are proving of limited use to advocates seeking to better understand the government's use of AI. Machine learning exemplifies trends toward privatization in government: One recent study of federal agencies' adoption of AI found that nearly half of the 157 use cases were provided through acquisitions from commercial vendors or partnerships between government and private enterprise.[32] Efforts to apply FOIA's disclosure obligations directly to source code and analogous records at the core of algorithmic governance confront head-on the pathologies of a system in which the private sector benefits from FOIA's entitlements while entirely avoiding its obligations.[33]

The law insulates the private sector from scrutiny in several respects.

First, FOIA only applies to records that an agency "controls."[34] This "control" requirement has often been interpreted to mean that technologies licensed to the government are beyond FOIA's reach.[35] In many cases, the vendor of an algorithmic system that is licensed to the government will continue to "control" the source code for the tool, leaving it outside of FOIA's reach. In agreements with vendors, governments also sometimes promise not to treat algorithmic tools like ordinary public records.[36] Nor do governments always control the training or input data that affect how machine-learning algorithms learn over time or generate their outputs.[37]

Second, even when an agency unambiguously "controls" a software system or data, regulated industries and private sector vendors have often succeeded in shielding business information from public disclosure, arguing that it constitutes trade secrets or confidential commercial information.[38] FOIA's Exemption 4 provides that the statute does not apply to "trade secrets and commercial or financial information obtained from a person and privileged or confidential."[39] The technology industry has resisted calls for algorithmic transparency, arguing that source code can be a highly protected trade secret.[40] Vendors also often argue that that data itself is proprietary.[41] The breadth of FOIA's protections for trade secrets and confidential business information is currently uncertain. On the one hand, the FOIA Improvement Act of 2016 amended FOIA to require that an agency may only withhold records when it "reasonably foresees" that release would cause harm, appearing to limit agencies' ability to withhold documents. On the other hand, a 2019 Supreme Court case, *FMI v. Argus Leader*, expanded the interpretation of the "confidential business information" exemption, fueling efforts to conceal private sector information.[42]

To be sure, expansive assertions of trade secrecy and confidentiality also impede transparency outside of the context of open government. When litigants have sought information about algorithms procured from private vendors to vindicate, for example, due process rights, vendors have asserted that the algorithms are trade secrets.[43] And in recent trade deals, Silicon Valley has successfully lobbied for provisions that prevent source-code disclosure.[44] Concerns about trade secrecy have motivated scholars to try to strike a pragmatic balance between disclosure obligations and legitimate commercial interests.[45]

FOIA's very design may have aggravated resistance to its use as a mechanism for understanding algorithmic governance. FOIA's widespread use by commercial entities as a form of business intelligence-gathering, and its policy of disclosure to any requester regardless of need, have likely contributed to aggressive efforts to maintain trade secrecy. Because FOIA requires public information to be made available to anyone on request, the potential costs of disclosure are high and incentivize firms to try to avoid it.

And because algorithmic systems—and the contexts in which they are used—are complex, the value of public disclosure is not always apparent. Many scholars of algorithmic accountability view FOIA-style public disclosure mandates as "naïve" at best and occasionally outright pernicious.[46] If a key problem with AI/ML systems is that they are too complex to be understood, the value of public disclosure is limited. Even sharp critics of algorithmic governance have evinced skepticism about transparency values. From a critical perspective, the idea of algorithmic transparency isn't just unattainable or unrealistic, but can actually serve as a dangerous distraction from broader accountability deficits, laden with "unexamined assumptions about the benefits of transparency, equating the ability to see inside a system with the power to govern it."[47] As Mike Ananny and Kate Crawford have argued, "transparency alone cannot create accountable systems"—attention must be paid to the political and social contexts in which technical systems operate.[48]

From transparency to accountability

Perhaps driven in part by FOIA's perceived failings, new approaches to "algorithmic transparency" are surfacing that prioritize technical solutions to opacity. At the same time as technology companies resist open-government, disclosure-based models of transparency, they have embraced a rich parallel debate about how to make AI *technically* transparent.[49] This debate is important: It holds the potential to improve the way AI tools work, and the way that they are perceived by their subjects and users. At the same time, the framing of algorithmic transparency risks marginalizing the value of public disclosure to participatory governance and democratic accountability.

Not surprisingly, the most aggressive reframing of transparency norms comes from industry. Technology vendors frame accountability and transparency as values best achieved through technology and the private sector itself rather than social, political, or legal principles that involve obligations toward the broader public. From the private sector's perspective, algorithmic transparency is a laudable goal that plays to companies' strengths: The private sector not only occupies a central role in making "transparency" technically achievable, but also in interpreting its core meaning.[50] Nor does the tech sector seriously address the potential clash between transparency values and its own interests in maintaining secrecy and confidentiality. Indeed, technology companies have successfully fought for provisions in trade agreements that broadly protect "source code" and "algorithms" from disclosure, even as they promise consumers that they will work to advance transparency, accountability, and trust.[51] This Janus-faced approach has garnered appropriate skepticism. As tech companies and interest groups hire new ethics officers and adopt new ethics guidelines to advance transparency and accountability, others have wondered whether the moves are just window dressing.[52] When it comes to accountability and transparency, many industry promises are so vague as to be meaningless.[53]

Private sector influence has thus yielded deeper and less obvious problems for transparency values beyond resistance to FOIA-style disclosure mandates. While FOIA does not extend to private contractors or vendors, a growing appetite for transparency and accountability has led the technology sector to repurpose these terms with a competing set of definitions. Unsurprisingly, this framing advances a different set of values than FOIA's emphasis on public participation and democratic self-governance.

Even outside of industry, technical approaches to algorithmic transparency have also adopted a narrower compass, avoiding implications for democratic governance. In particular, technical approaches to "explainability" and "algorithmic accountability" largely focus on the question of how AI can provide certain key information about how it functions, rather than the question of what kinds of public information democratic governance requires.[54]

Indeed, some accountability advocates have turned their noses up at public disclosure obligations, arguing instead for more limited, alternative "transparency" mechanisms.[55] In one influential article, several authors pushed back against the idea that transparency can be a remotely realistic or effective mechanism for promoting accountability.[56] Instead, Kroll et al. suggest that "accountability" means determining why a feature is necessary and explaining how its use satisfies policy goals.[57]

This narrower version of accountability keeps significant discretion in the hands of algorithm developers who can satisfy "accountability" demands by explaining their procedures without jeopardizing trade secrecy or calling into question their other commercial interests. Having defined "accountability" in this way, it follows that a range of options for promoting transparency and accountability—in particular, disclosure—are off the table, namely because they don't serve this particular *kind* of accountability-as-verifiability. In fact, this account seems to suggest that significant secrecy can attend algorithmic decision making, so long as the subjects of decisions can be adequately reassured that the rules were followed.[58] Strikingly, this version of accountability says nothing about how to achieve democratic oversight or public participation, or otherwise guarantee that an algorithm is ultimately "accountable" to the public.[59] The problem, then, is not simply that the private sector does not want to disclose information about AI to the public, but that the public is notably absent from much of this robust discussion about how best to design and implement algorithmic accountability or transparency from a technical perspective.

Instead, new ideas about algorithmic accountability and transparency focus nearly exclusively on how technology providers can ensure that their products don't violate individual rights. An important related literature explores how individuals might be able to challenge algorithmic decisions that affect them, increasingly seeking "explainability" for the outcomes of automated decisions.[60] The so-called "right to explanation" focuses on an individual right to have the outcome of an algorithmic process explained in an intelligible way. In theory, at least, such a right can be vindicated without jeopardizing trade secret or other proprietary interests—a perfect balancing of the vendor's commercial interest against the data subject's dignitary one.[61]

Advocates of "explainability" have thus successfully expanded the project of algorithmic transparency and accountability beyond mere technical transparency. Inadvertently, however, in so doing they have reframed the project of algorithmic accountability as being primarily about individual rights.[62] As Margot Kaminski has noted, several of the most compelling approaches to algorithmic accountability combine the individual rights approach with a more systemic approach to AI governance.[63] Increasingly, scholars are beginning to explicitly consider the role of administrative oversight and public governance in algorithmic accountability.[64] Meanwhile, others continued to highlight transparency as a sometimes useful mechanism for ensuring accountability.[65] Still others have adopted more of a political conception of accountability.[66]

Whatever FOIA's drawbacks at facilitating democratic participation—and as articulated above, there are many—these private sector norms of accountability and transparency are even worse. Instead of positioning transparency as a tool of democratic participation, transparency is a minimal obligation to ensure that individuals know how and when decisions are made about them. Instead of seeing transparency as a right that effectuates a mechanism for checking institutional malfeasance and power, transparent AI is a promise that only powerful institutions are in a position to make.[67]

II. TRANSPARENCY IN HIGH-STAKES SETTINGS

IN HIGH-STAKES SETTINGS with lives and livelihoods on the line, promises to use technology in ways that are "transparent" and "accountable" just don't hold up. Consider how, in 2007, Indiana privatized and automated its system for applying for welfare benefits, resulting in more than a million denials—many erroneous.[68] Or how, in 2013, the Michigan Unemployment Insurance Agency asked third-party technology companies to automate the state's application for unemployment benefits. When the automation malfunctioned, tens of thousands of people were wrongfully accused of fraud, and many had their wages garnished or civil penalties imposed.[69] Or how, in 2015, the West Virginia Department of Health and Human Services relied on a proprietary algorithm to slash critical Medicaid benefits, leaving disabled adults across the state without vital home-based care and, instead, institutionalized in care facilities or group homes.[70]

In circumstances like these, democracy demands more than promises of explainability and ethical behavior. In order to make informed decisions about governance today, the public needs much more information about how these technologies operate. Instead, however, that information remains in private hands, often as the result of efforts to conceal key information from public view.

Nowhere is that dynamic more evident than in the context of criminal law enforcement, where automated decision making comes with particularly high stakes.[71] Algorithms and artificial intelligence are transforming policing, enabling law enforcement to cheaply and easily use facial recognition, gait recognition, license plate readers, gang databases, social media surveillance, predictive policing, and a range of other data-rich tools and methods. Algorithms are also transforming pretrial release, sentencing, and parole hearings.[72] And proprietary software is increasingly used in generating evidence used against defendants at trial.[73]

It is tempting to think of criminal law enforcement algorithms as the quintessential example of "public" algorithms. But the sizable footprint of private vendors in this sector has posed serious obstacles to efforts to make policing more transparent and more accountable, as Elizabeth Joh has noted.[74] For instance, law enforcement has obtained predictive policing algorithms from vendors such as Palantir, the shadowy surveillance company that supplies technology to federal, state, and local governments. When activists and advocates have sought information about these technologies, agencies have sometimes claimed that releasing audits, test results, and other information would violate nondisclosure agreements and jeopardize trade secrets.[75] Similarly, private vendors have invoked trade secrecy to justify withholding the source code of a risk assessment used to sentence an individual to prison.[76]

As widespread resistance to racist police violence and repression continues to sweep the nation, police technologies such as facial recognition, predictive policing, and other surveillance technologies are coming under sustained scrutiny. Consider, for example, efforts to shed light on facial recognition and other surveillance mechanisms. Facial recognition is a form of biometric surveillance that identifies distinctive aspects of an individual's facial structure and screens those characteristics against a database of photographs. A majority of states use facial recognition within their departments of motor vehicles, and 26 states permit law enforcement to screen photographs of potential criminal suspects against their DMV's database of drivers' license photos.[77]

One major concern about facial recognition involves the potential for racial and gender bias.[78] A recent National Institute of Standards and Technology (NIST) study examining the accuracy of facial recognition software in identifying people of varied sex, age, and racial background found that the software demonstrated higher false positive rates—the frequency of misidentifying a face as a match—for Black and Asian faces than white faces.[79] Facial recognition technology also performs less accurately for "female" faces than for "male" faces, and poorer still for dark-skinned female faces.[80]

A significant portion of advocacy on facial recognition has centered on the role of private contractors, among which Amazon, owner and operator of the Ring Video Doorbell surveillance system, is perhaps the most visible.[81] While the company sells its doorbell cameras directly to consumers, Amazon also partners with hundreds of law enforcement agencies around the country to share access to the footage and to encourage more widespread consumer adoption.[82] Amazon is also reportedly considering how to build facial recognition into its Ring systems.[83]

Advocates have likely grown concerned about Clearview AI, a company that uses a facial recognition algorithm to cross-reference a photo of an individual against a library of images scraped from social media sites such as Facebook and Twitter.[84] In early 2020, Kashmir Hill reported that over 600 law enforcement agencies had begun using Clearview, often without publicly disclosing it. While Clearview later announced it would stop providing the technology to private enterprise, it has continued to supply it to law enforcement agencies.[85] Other vendors have proven more susceptible to public backlash, announcing a moratorium on the sale of facial recognition technology to law enforcement.[86]

Efforts to make policing technologies transparent and accountable to the public do not stop at technocratic transparency, but rather force information into the open as part of a strategy to democratize law enforcement, radically shrink its footprint in American cities, and create community-led alternatives.[87] Strategically, activists eager to reform criminal law enforcement and reduce its footprint on American life have simultaneously harnessed the existing framework of open government and recognized its limitations, pushing for new and different forms of transparency and accountability. While private vendors themselves are beyond the reach of FOIA or its state equivalents, freedom of information laws have proven essential in unveiling the relationships between vendors and agencies, and in stimulating public debate. Activists have focused a substantial amount of energy on bringing secretive police technologies into the public eye, subjecting them to public oversight, and questioning the legal structures that enable algorithmic policing to thrive.

Access to information is essential to be able to evaluate the potential value—and costs—of automated decision making in the context of criminal law enforcement. As Bennett Capers has suggested, new technologies of policing, and widespread surveillance in particular, may actually reduce the kinds of racial inequality and profiling to which the Supreme Court has historically turned a blind eye.[88] And Andrew Ferguson has described how broad systems of predictive policing might also be used to glean critical information to hold police accountable—what he calls "blue data."[89] This guarded optimism about the potential value of algorithmic criminal law enforcement comes with a giant caveat: It only holds if the technologies of policing themselves do not exhibit "implicit biases" or "suffer from unconscious racism."[90] Indeed, critics of these law enforcement tools see them as nothing more than a way to cast racist policing practices in an "objective" light.[91]

The integral role of technology in expanding and bolstering law enforcement power underscores the limitations of a technocratic form of algorithmic transparency. Even carefully crafted algorithmic accountability regimes are unlikely to resolve deep-rooted concerns about whether facial recognition algorithms are truly just or fair. The remedy that the subjects of algorithmic policing want is usually not going to be an "explanation" of a decision, an articulation of the general rule, or the disclosure of a data set. They want the decision not to take place at all.[92] To put it another way, democracy requires us not only to ensure that AI systems are accountable, transparent, explainable, ethical, and all the rest, but also to ensure that the public gets to determine whether they are used—and how to govern them.[93]

III. TOWARD A NEW ALGORITHMIC TRANSPARENCY

EVEN AS PRIVATE TECHNOLOGY vendors play an increasingly relevant and important role in public governance, our open-government frameworks permit them to operate without public scrutiny. Partly because of this transparency gap, ideals of transparency and accountability for algorithms are being reimagined by scholars and the private sector alike. While these contributions are important and significant, they share one major shortcoming: They fail to fully acknowledge, and therefore to adequately protect, values of democratic participation and public governance. Practically speaking, freedom of information laws share the same shortcomings, failing to vindicate their promise of participatory governance.

The result is a serious accountability deficit. The law must adapt to the challenges that automated decision making poses to public transparency and accountability. But rather than deferring to private authority or technical measures of transparency, the law should protect structures of accountability that make real the promise of public participation and democratic accountability.

The project of democratizing algorithms will require a renewed commitment to public oversight structures and democratic participation. We should reaffirm the values that underpin transparency law itself—self-governance, improving government through oversight, and free expression—as sources of renewed democratic control. These principles point to a possible understanding of the kinds of information about automated decision-making systems that we might require be disclosed to the public.[94]

For now, one concrete change would make a significant difference: the procurement and use of proprietary algorithmic decision-making technologies in government should be brought under democratic control. It might seem somewhat ironic to reappropriate the legal frameworks of the outsourcing process in order to bring the rule of law to bear on automated decision making.[95] But agencies, as contracting entities, are in a position to demand and enforce contractual terms in the public interest in concrete ways.[96] In light of the shrinking public role in governing algorithms, reaffirming that public agencies ultimately set the agenda for automated decision making is a significant step forward.

What does that look like? Successful efforts to impose ex ante oversight and control of police technologies are growing in number. Laws requiring legislative approval for the acquisition of any new surveillance technology and for the publication of impact assessments and policies on surveillance use have been enacted in Nashville, Tennessee; Seattle, Washington; and Cambridge, Massachusetts.[97] The ACLU has drafted a model bill for ex ante oversight of surveillance technology intended for widespread adoption.[98] Naturally, these efforts have, on occasion, met with significant resistance from law enforcement agencies.[99] In the present moment, however, they seem to be growing in number and in volume.

One recent victory deserves particular mention. In April 2020, Washington enacted a statute that forbids government agencies to "develop, procure or use" facial recognition technology without first preparing a detailed "accountability report"—which must be subject to public review and comment, including at least three community meetings, before being finalized.[100] In theory, at least, the ex ante notice and comment framework set forth in Washington's law will provide ample opportunity for the public to weigh in on potential issues with bias, accuracy, and trade secrecy for facial recognition software. In this respect, the statute parallels algorithmic impact assessments, which provide an opportunity for agencies to "engage the public and proactively identify concerns, establish expectations, and draw on expertise and understanding from relevant stakeholders."[101] This approach may not be perfect. Without reform to procurement rules and practices, which allow vendors to hide behind a veil of trade secrecy, there is no guarantee that an "impact assessment" will tell us anything meaningful about a technology, nor that it won't be co-opted by the vendors it seeks to expose.[102] Compared, however, with relatively meaningless assurances from the technology sector, this is an improvement.

At a bare minimum, statutes should limit agencies' ability to enter into vendor contracts that purport to circumvent open records obligations. As a matter of public policy—and as a matter of transparency law—the prevalent practice of contracting for secrecy is questionable at best.[103] Recent legislation shows forward progress on this ground: In September 2019, Rep. Mark Takano introduced the Justice in Forensic Algorithms Act, which would amend the Federal Rules of Evidence to bar using the trade secret privilege alone to prevent disclosure of evidence to criminal defendants. A similar statute enacted in 2019 in Idaho requires pretrial risk assessment algorithms to be "transparent," and specifies that "no builder or user of a pretrial risk assessment algorithm may assert trade secret or other protections in order to quash discovery in a criminal matter by a party to a criminal case."[104]

While the focus on criminal law enforcement algorithms is understandable and commendable, these initiatives do not go far enough. For one thing, they do not even begin to address facial recognition, predictive policing, license plate readers, or the myriad other technologies in daily use in American police departments. A more cross-cutting strategy is justifiable.

Rather than addressing trade secrecy on a piecemeal basis, reforms to procurement policy could disfavor trade secrecy for proprietary tools of automated decision making more broadly. As advocates at AI Now have suggested, states and municipalities could reform the law of government contracts to account for other social interests beyond low bids.[105] Rather than simply accepting the lowest bidder, contracting entities could consider adherence to other important values, including openness. For instance, procurement law could be amended to provide that a contracting government entity must consider whether a bidder relies on trade secrecy to shield its algorithms from public disclosure. In many states, consideration of these values would require a change to the state's procurement law.[106]

Contracting entities, in considering vendors' claims to openness, should take into account both outright invocations of trade secrecy and proposals to circumvent government transparency obligations. But government contracts should also encourage vendors to commit to other kinds of open standards, and in particular those developed through rigorous, public, multi-stakeholder processes. This strategy could borrow from the federal government's source-code policy (FSCP), which seeks to achieve "efficiency, transparency, and innovation through reusable and open source software."[107] The FSCP was intended to constrain federal agencies' acquisition of custom-developed computer code when a viable existing federal or commercial solution provides an alternative. Notably, the FSCP also articulates a preference for publicly developed code and instructs agencies to "consider utilizing open standards whenever practicable in order to increase the interoperability of all Government software solutions."[108]

Open standards for artificial intelligence are still nascent. In 2019, an executive order, “Maintaining American Leadership in Artificial Intelligence” (EO 13859), instructed NIST to prioritize federal engagement in the development of AI standards. NIST’s role as a venerable standards organization bodes well for this process. Even NIST acknowledges, however, that the technology may be too new for standards development to make sense.[109]

Despite this early stage, however, active government involvement in fostering standards-setting for emerging technology makes good sense. In this vein, policy could incentivize vendors to participate in multistakeholder standards-setting activities to spur innovation around open standards.[110]

Second, new forms of proactive disclosure may be necessary to make sense of automated decision making. In this respect, contracting agencies might take their cue from efforts to promote open science. In 2013, the White House issued a directive requiring agencies to develop plans for sharing data generated from publicly funded research.[111] Supporters believe that requiring data-sharing will foster open science and produce new and innovative research.

A similar move could foster openness in automated decision making. If procuring entities required the recipients of public funds (whether those funds were received through grants or through contracts) to proactively share critical information about how their technologies function, it would not only create valuable synergies for researchers but also add some much-needed scientific rigor to an industry that some have accused of selling pure “snake oil.”[112]

Open AI development may raise security and privacy concerns.[113] Similar criticisms have been lodged against the open-data policy—scientists worry about “rigid standards” for data-sharing, and privacy advocates are rightly concerned about the privacy of participants in studies such as clinical trials.[114] I leave for another day a discussion of the precise contours that might or might not be appropriate here.

A third avenue, worth considering, is whether the state itself has a role to play, not just in auditing and monitoring automated decision making, but also in facilitating public participation. David Engstrom and Daniel Ho have recently argued that agencies should engage in “prospective benchmarking,” in which they would compare a random sample of decisions generated by

AI decision-making tools against the same cases, decided by humans.[115] One concern, naturally, is that agencies convinced that AI provides a more efficient and less expensive decision-making system might be disinclined to look closely at evidence that might undermine that belief, or to publicize negative results. And, at least at the state and local level, it may be unrealistic to expect this level of analysis from under-resourced agencies without much technical expertise. But prospective benchmarking might provide an avenue through which public participation could be broadened and made more meaningful; the results of prospective benchmarking, for example, might be published and made subject to notice and comment, facilitating both public understanding and participation.

Cities and states, too, can do much more to engage the public in questions about algorithmic decision making. Policies that require public notice and comment, or community meetings before acquiring new surveillance technologies point to one potential path forward. Cities and states can affirmatively commit to disclosing information about algorithmic systems in current use and soliciting public input each time a new algorithmic decision system is adopted.

One path forward is through the adoption of "AI registers." AI registers are essentially formats for documenting "the decisions and assumptions that were made in the process of developing, implementing, managing and ultimately dismantling an algorithm."[116] The cities of Helsinki and Amsterdam have both recently begun to roll out AI registers, websites that they use to host and make available information about certain kinds of artificial intelligence systems in current use.[117] In a similar development, after New York City enacted the Public Oversight of Surveillance Technology Act in 2020, the New York Police Department began to publish impact and use policies on its website for notice and comment for each "surveillance technology" in use, although the information is not nearly as detailed, user-friendly, or granular as that in the Helsinki or Amsterdam registers.[118]

These transparency-enhancing practices are, of course, not without cost. Indeed, even apparently well-meaning policy interventions have sometimes foundered simply because it is too difficult to assemble a full list of every AI system in place. Consider the New York City Automated Decision Systems Task Force, which was created in 2017 to "come up with recommendations for government use of" automated decision systems, but was stymied when the city would not disclose which automated decision systems it was, in fact, using.[119] Despite the short-term costs, however, the long-term benefits might include enhancing buy-in by the public and helping to air potential problems with algorithmic systems earlier, rather than later.

Finally, civil society institutions and press outlets can play a meaningful role in ensuring that key information about automated decision making reaches the public. In Europe, institutions such as AlgorithmWatch and the Ada Lovelace Institute fulfill important watchdog and advocacy functions for automated decision systems. In the United States, the closest analogue is likely the AI Now Institute, a university-based think tank that performs similar roles. Increasingly, specialized press outlets such as The Markup and even Consumer Reports are also conducting investigative reporting on algorithmic-decision systems and ensuring that vital information finds an audience. Ultimately, increasing reliance upon automation means that journalists, press institutions, and civil society will need to fight to ensure public access to the new methods of governance.

Importantly, these approaches to instantiating algorithmic transparency are neither about individual rights nor about technocratic transparency. Instead of placing key information about how algorithms work in the hands of auditors or agencies that cannot disclose it to the public, these public-oriented protections democratize information and share it widely.

In this sense, the proposals might come under criticism for both doing too much and too little. Critics might fear that impediments to secrecy and requirements for widespread disclosure would undermine competition by discouraging vendors from investing in developing automated decision-making tools and thus ultimately stifle innovation. But—as is the case for policing—many of these vendors market their products primarily or exclusively to the government. Companies for whom government agencies are a major customer are unlikely to be deterred by more rigorous contracting requirements.

Critics might also (rightly) suggest that information disclosure is not enough for real accountability. Average members of the public are unlikely to be able to make use of the disclosures I describe above. This "thin" version of transparency, then, does not address the same concerns as a right to an explanation or thicker accountability mechanisms might.

Yet there are two key benefits to investing in information disclosure. First, disclosure requirements might create a "market for expertise" that ultimately empowers the press and civil society to engage in the kinds of newsgathering and rigorous analysis that stimulate public oversight. [120] Already, specialized nonprofit press outlets such as The Markup, The Appeal, and The Marshall Project are developing substantial expertise reporting on the instruments of algorithmic governance and their impact on criminal law enforcement.[121]

Second, while transparency is not sufficient to guarantee accountability—and does not inevitably lead to accountability—it is a vital precondition to accountability-enhancing efforts. As the experience with efforts to reform criminal law enforcement shows, the power to compel government to reveal how police use AI is an essential part of a broader reckoning with police power and the technology vendors that amplify it.

Information-forcing approaches, then, are an admittedly incomplete way of addressing algorithmic accountability. But legal structures that ensure that algorithmic governance works for the *public*, rather than for private enrichment, are integral to democracy. The question of how algorithmic governance might be made transparent thus raises broader questions both about the role of transparency in democratic governance—and about the role of democracy in governing algorithms.

NOTES

[1] AI is a notoriously slippery term. In this essay, I am talking about software systems that can interpret large amounts of data and determine how to act in order to accomplish an articulated goal. *See* Eur. Comm'n High Level Expert Grp. on A.I., Ethics Guidelines for Trustworthy AI, at 36 (Apr. 8, 2019). *See also* David Freeman Engstrom et al., *Government by Algorithm: Artificial Intelligence in Federal Administrative Agencies*, SSRN Elec. J. (2020).

[2] *See, e.g.*, Joshua A. Kroll et al., *Accountable Algorithms*, 165 U. Pa. L. Rev. 633 (2017); Deborah Hellman, *Measuring Algorithmic Fairness*, 106 Va. L. Rev. 811 (2020); Florian Cech, *Beyond Transparency: Exploring Algorithmic Accountability, in* Companion of the 2020 ACM International Conference on Supporting Group Work 11–14 (2020); Nicholas Diakopoulos, *Accountability in Algorithmic Decision Making*, 59 Commc'n ACM 56 (2016); Mike Ananny & Kate Crawford, *Seeing Without Knowing: Limitations of the Transparency Ideal and its Application to Algorithmic Accountability*, 20 New Media & Soc'y 973 (2018); Margot E. Kaminski, *Binary Governance: Lessons from the GDPR's Approach to Algorithmic Accountability*, 92 S. Cal. L. Rev. 1529 (2018–2019); Solon Barocas et al., *Big Data, Data Science, and Civil Rights*, arXiv:1706.03102 (June 9, 2017), http://arxiv.org/abs/1706.03102 [https://perma.cc/K2B7-8VN4]; Manish Raghavan et al., *Mitigating Bias in Algorithmic Hiring: Evaluating Claims and Practices*, arXic:1906.09208 (June 21, 2019), https://arxiv.org/abs/1906.09208 [https://perma.cc/YKX3-8YTT]; Reuben Binns, *Algorithmic Accountability and Public Reason*, 31 Phil. & Tech. 543 (2018); Brent Daniel Mittelstadt et al., *The Ethics of Algorithms: Mapping the Debate*, Big Data & Soc'y, Dec. 2016.

[3] Jenna Burrell, *How the Machine "Thinks": Understanding Opacity in Machine Learning Algorithms*, Big Data & Soc'y, Jan.–June 2016.

[4] Miles Brundage et al., *Toward Trustworthy AI Development: Mechanisms for Supporting Verifiable Claims*, arXiv:2004.07213 (Apr. 15, 2020), https://arxiv.org/abs/2004.07213 [https://perma.cc/RQ79-LNGJ]; *see also* Inioluwa Deborah Raji et al., *Saving Face: Investigating the Ethical Concerns of Facial Recognition Auditing*, arXiv:2001.00964 (Jan. 3, 2020), https://arxiv.org/abs/2001.00964 [https://perma.cc/4DZV-VNHX].

[5] Kaminski, *supra* note 2; Sandra Wachter, Brent Mittelstadt & Chris Russell, *Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR*, 31 Harv. J. L. & Tech. 841 (2017); Andrés Páez, *The Pragmatic Turn in Explainable Artificial Intelligence (XAI)*, 29 Minds & Mach.'s 441 (2019); Andrew D. Selbst & Solon Barocas, *The Intuitive Appeal of Explainable Machines*, 87 Fordham L. Rev. 1085 (2018); Joshua A. Kroll & Deven R. Desai, *Trust But Verify: A Guide to Algorithms and the Law*, 31 Harv. J. L. & Tech. 1 (2017).

[6] This project is thus in conversation with legal scholars seeking to "democratize" and redistribute power over law enforcement and other government institutions as much as it is technology scholars seeking to bolster participation in tech governance. *See, e.g.*, Jocelyn Simonson, *Democratizing Criminal Justice Through Contestation and Resistance*, 111 Nw. U. L. Rev. 1609 (2016–2017); Dorothy E. Roberts, *Democratizing Criminal Law as an Abolitionist Project*, 111 Nw. U. L. Rev. 1597 (2016–2017); Amna A. Akbar, *Toward a Radical Imagination of Law*, 93 N.Y.U. L. Rev. 405 (2018); *see also* Gregory Falco, *Participatory AI: Reducing AI Bias and Developing Socially Responsible AI in Smart Cities, in* 2019 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC) 154–58 (2019); Donald Martin, Vinodkumar Prabhakaran, Jill Kuhlberg, Andrew Smart & William S. Isaac, *Participatory Problem Formulation for Fairer Machine Learning Through Community Based System Dynamics Approach* 6 (May 15, 2020), https://arxiv.org/abs/2005.07572 [https://perma.cc/2SY5-RFSD].

[7] *See, e.g.*, Rory Van Loo, *Rise of the Digital Regulator*, 66 Duke L. J. 1267 (2017); Rory Van Loo, *The Corporation as Courthouse*, 33 Yale J. on Regul. 547 (2016); Rory Van Loo, *The New Gatekeepers: Private Firms as Public Enforcers*, 106 Va. L. Rev. 56 (2020); Kate Klonick, *The New Governors: The People, Rules, and Processes Governing Online Speech*, 131 Harv. L. Rev. 1598 (2018); Jack M. Balkin, *Free Speech in the Algorithmic Society: Big Data, Private Governance,*

and New School Speech Regulation, 51 U.C. Davis L. Rev. 1149 (2018); Kristen E. Eichensehr, *Digital Switzerlands*, 167 U. Pa. L. Rev. 665 (2019); Kate Crawford & Jason Schultz, *AI Systems As State Actors*, 119 Colum. L. Rev. 1941 (2019); Alan Z. Rozenshtein, *Surveillance Intermediaries*, 70 Stan. L. Rev. 99 (2018).

[8] Martha Minow, *Public and Private Partnerships: Accounting for the New Religion*, 116 Harv. L. Rev. 1229 (2003); Jody Freeman, *The Private Role in Public Governance*, 75 N.Y.U. L. Rev. 543 (2000); Kimberly N. Brown, *We the People, Constitutional Accountability, and Outsourcing Government*, 88 Ind. L. J. 1347 (2013); Jon D. Michaels, *Privatization's Pretensions*, 77 U. Chi. L. Rev. 717 (2010); Alfred C. Aman, *Privatization and the Democracy Problem in Globalization: Making Markets More Accountable Through Administrative Law*, 28 Fordham Urb. L. J. 1477 (2001).

[9] Dep't of Air Force v. Rose, 425 U.S. 352, 361 (1976) (quoting Rose v. Dep't of Air Force, 495 F.2d 261, 263 (2d Cir. 1974)).

[10] Margaret B. Kwoka, *Deferring to Secrecy*, 54 B.C. L. Rev. 185, 197 (2013).

[11] Christina Koningisor, *Transparency Deserts*, 114 Nw. U. L. Rev. 1461, 1475 (2020).

[12] The Freedom of Information Act, 5 U.S.C. § 552(b)(1)–(9) (2018).

[13] *Id.* 5 U.S.C. § 552(b)(1)-(9) (setting forth nine exceptions); Vaughn v. Rosen, 484 F.2d 820, 823 (D.C. Cir. 1973) (exemptions are to be "construed narrowly" in accordance with a policy of "maximum access"); *but see* Food Mktg. Inst. v. Argus Leader, 139 S.Ct. 2356, 2366 (2019) ("[A]s we have explained in connection with another federal statute, we 'normally have no license to give [statutory] exemption[s] anything but a fair reading.'") (*quoting* Encino Motorcars, LLC v. Navarro, 584 U. S. ___, ___ (2018) (slip op., at 9)).

[14] *Id.* 5 U.S.C. § 552(B)(1), (3), (4), (5), (6), (7).

[15] Margaret B. Kwoka, *FOIA, Inc.*, 65 Duke L. J. 1361, 1371 (2015–2016).

[16] Rory Van Loo, *Regulatory Monitors: Policing Firms in the Compliance Era*, 119 Colum. L. Rev. 369, 381 (2019) (describing regulatory monitors' ability to compel firms to report or disclose information).

[17] David E. Pozen, *Freedom of Information Beyond the Freedom of Information Act*, 165 U. Pa. L. Rev. 1097, 1114–15 (2017); Mark Fenster, *The Opacity of Transparency*, 91 Iowa L. Rev. 885, 917–18 (2005–2006).

[18] Laura A. Dickinson, *Privatization and Accountability*, 7 Ann. Rev. L. & Soc. Sci. 101, 109 (2011); *see also* Henry Farrell, *Privatization as State Transformation, in* Privatization: Nomos LX 185, 185 (Jack Knight & Melissa Schwartzberg eds., 2019) ("[V]isibility and accountability are occluded by a dense cobweb of relationships.").

[19] Paul C. Light, The Government-Industrial Complex, 59 (2019); David H. Rosenbloom & Suzanne J. Piotrowski, *Outsourcing the Constitution and Administrative Law Norms*, 35 Am. Rev. of Pub. Admin. 103, 107 (2005).

[20] *See, e.g.*, Minow, *supra* note 8; Paul R. Verkuil, *Public Law Limitations on Privatization of Government Functions*, 84 N.C. L. Rev. 397 (2005–2006); Freeman, *supra* note 8; Dickinson, *supra* note 18; Kimberly N. Brown, *Government by Contract and the Structural Constitution*, 87 Notre Dame L. Rev. 491 (2011–2012); Michaels, *supra* note 8.

[21] NASA STS-107 News Records Released under Freedom of Information Act, https://www.nasa.gov/columbia/foia/index.html [https://perma.cc/N33X-9SNX] (last visited Apr. 6, 2021).

[22] Rosenbloom & Piotrowski, *supra* note 19, at 106.

[23] David E. Pozen, *Transparency's Ideological Drift*, 128 Yale L. J. 100, 151 (2018–2019).

[24] K. Sabeel Rahman, *(Re)Constructing Democracy in Crisis*, 65 UCLA L. Rev. 1552, 1566 (2018).

[25] Fenster, *supra* note 17, at 949; Pozen, *supra* note 23, at 1115 (describing how "the evils of excessive secrecy are associated, legally and symbolically, with the public sector alone").

[26] Kenneth Culp Davis, *The Information Act: A Preliminary Analysis*, 34 U. Chi. L. Rev. 761, 765 (1967) ("The Act never provides for disclosure to some private parties and withholding from others.").

[27] Pozen, *supra* note 23, at 1117.

[28] Kwoka, *supra* note 15 at 1380.

[29] Koningisor, *supra* note 11 (describing obstacles to disclosure in the state and local context).

[30] *See, e.g.*, Hannah Bloch-Wehba, *Access to Algorithms*, 88 Fordham L. Rev. 1265 (2020); Robert Brau-

neis & Ellen P. Goodman, *Algorithmic Transparency for the Smart City*, 20 Yale J. L. & Tech. 103 (2018).

[31] NRDC v. EPA, 954 F.3d 150, 158 (2d Cir. 2020) (rejecting agency's claim that its Optimization Model for Reducing Emissions of Greenhouse Gases for Automobiles (OMEGA) was protected under the deliberative process privilege).

[32] Engstrom et al., *supra* note 1, at 88.

[33] Katherine Fink, *Opening the Government's Black Boxes: Freedom of information and algorithmic accountability*, 21 Info., Commc'n & Soc'y 1453 (2018) at 1462.

[34] Bloch-Wehba, *supra* note 30, at 1299-1300.

[35] *See, e.g.*, Tax Analysts v. U.S. Dep't of Justice, 913 F. Supp. 599, 607 (D.D.C. 1996), Aff'd Sub Nom., Tax Analysts v. Dep't of Justice, 107 F.3d 923 (D.C. Cir. 1997).

[36] Bloch-Wehba, *supra* note 30, at 1286 (describing memoranda of understanding with the Arnold Foundation).

[37] Lee Rainie & Janna Anderson, *Code-Dependent: Pros and Cons of the Algorithm Age* 75 (Pew Research Center 2017).

[38] Brauneis & Goodman, *supra* note 30.

[39] 5 U.S.C. § 552(b)(4).

[40] Kartik Hosanagar & Vivian Jair, *We Need Transparency in Algorithms, But Too Much Can Backfire*, Harv. Bus. Rev., 2018, https://hbr.org/2018/07/we-need-transparency-in-algorithms-but-too-much-can-backfire [https://perma.cc/8JXT-EU26]; see also Rebecca Wexler, *Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System*, 70 Stan. L. Rev. 1343 (2018); Rainie & Anderson, *supra* note 37, at 19; Brauneis & Goodman, *supra* note 30, at 153.

[41] *See, e.g.*, Bloch-Wehba, *supra* note 30, at 1283–84 (describing how ShotSpotter, a gunshot detection firm, has claimed that the data it collects is proprietary).

[42] Food Mktg. Inst. v. Argus Leader, 139 S.Ct. 2356 (2019).

[43] *See, e.g.*, Hous. Fed'n of Tchr's, Loc. 2145 v. Hous. Indep. Sch. Dist., 251 F. Supp. 3d 1168 (S.D. Tex. 2017); State v. Loomis, 881 N.W.2d 749, 769-71 (Wis. 2016) (upholding the use of proprietary risk assessment algorithms at sentencing); *see also* Thomas Claburn, *Accused murderer wins right to check source code of DNA testing kit used by police*, Reg. (Feb. 4, 2021), https://www.theregister.com/2021/02/04/dna_testing_software/[https://perma.cc/ZV8Q-75VQ].

[44] Kate Kaye, *How the Tech Industry Coordinated to Squelch Algorithm Transparency in the New NAFTA Deal*, Red Tail Media (Nov. 8, 2018), https://redtailmedia.org/2018/11/08/how-the-tech-industry-prevented-algorithm-transparency-in-nafta-2-0/ [https://perma.cc/3LHZ-AGJH].

[45] Wexler, *supra* note 40; Selbst & Barocas, *supra* note 4, at 1092; Natalie Ram, *Innovating Criminal Justice*, 112 Nw. U. L. Rev. 659, 717–18 (2017–2018).

[46] Lilian Edwards & Michael Veale, *Slave to the Algorithm: Why a Right to an Explanation Is Probably Not the Remedy You Are Looking For*, 16 Duke L. & Tech. Rev. 18, 43 (2017–2018), citing Kroll et al., *supra* note 2 at 638–39 (describing source code as "illegible"); *see also* Ananny & Crawford, *supra* note 2 at 6–8 (describing the drawbacks of transparency).

[47] *Id.*

[48] *Id.*

[49] In a sense, this development parallels the evolution of "privacy by design," the concept that "privacy must become integral to organizational priorities, project objectives, design processes, and planning operations." Ann Cavoukian, Privacy By Design: The Seven Foundational Principles 2 (2011). As Woody Hartzog points out, privacy by design "is often used to refer to self-regulatory measures taken by companies ... a chorus of industry voices champions the promise of privacy by design, but the conversation ends when the role of law and regulators is raised." Woodrow Hartzog, Privacy's Blueprint 5 (2018); *see also* Ari Ezra Waldman, *Designing Without Privacy*, 55 Hous. L. Rev. 659, 681–85 (2017) (demonstrating that technologists and lawyers tasked with incorporating privacy into the design process adopted narrow visions of privacy's meaning).

[50] *See, e.g.*, IBM, *IBM's Principles for Trust and Transparency*, IBM (June 2018), https://www.ibm.com/policy/wp-content/uploads/2018/06/IBM_Principles_SHORT.V4.3.pdf [https://perma.cc/W3T8-M2TH] ("IBM will make clear: when and for what purposes AI is being applied.").

[51] *See, e.g.*, Agreement Between the United States

of America, the United Mexican States, and Canada, art. 19.16, July 1, 2020, (broadly barring source code disclosure requirements); EXPLAINABLE AI, https://cloud.google.com/explainable-ai [https://perma.cc/JYQ8-TZE4] (last visited Apr. 16, 2021) (marketing the relationship between "explainable AI" and "end-user trust").

[52] Kara Swisher, *Who Will Teach Silicon Valley to Be Ethical?*, N.Y. TIMES (Oct. 21, 2018), https://www.nytimes.com/2018/10/21/opinion/who-will-teach-silicon-valley-to-be-ethical.html [https://perma.cc/B4K2-DK9L].

[53] *See, e.g.*, ARTIFICAL INTELLIGENCE AT GOOGLE: OUR PRINCIPLES, https://ai.google/principles/ [https://perma.cc/DE48-55FX] (last visited Apr. 16, 2021) (promising that Google's AI will be "accountable to people").

[54] Archon Fung, *Infotopia: Unleashing the Democratic Power of Transparency*, 41 POL. & SOC'Y 183, 185 (2013) (noting that democracy requires "the public provision of information").

[55] *See* Kaminski, *supra* note 2, at 1533 (noting that public-facing accountability has become one of the "straw men" of debates).

[56] Kroll et al., *supra* note 2, at 658–60.

[57] *Id.* at 653–54.

[58] *Id.* at 673 (discussing benefits of ensuring procedural regularity without knowing how a system works).

[59] *Id.* at 678.

[60] Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249 (2007) (introducing the concept of "technological due process"); Wexler, *supra* note 40; Katherine J. Strandburg, *Adjudicating with Inscrutable Decision Tools, in* MACHINES WE TRUST: GETTING ALONG WITH ARTIFICIAL INTELLIGENCE (Marcello Pelillo & Teresa Scantamburlo eds., 2020); Sandra Wachter, Brent Mittelstadt & Chris Russell, *Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR*, 31 HARV. J. L. & TECH. 841 (2017); Tim Miller, *Explanation in Artificial Intelligence: Insights from the Social Sciences*, ARXIV:1706.07269 (Aug. 15, 2018) http://arxiv.org/abs/1706.07269 [https://perma.cc/EBG8-728N]; Margot E. Kaminski, *The Right to Explanation, Explained*, 34 BERKELEY TECH. L. J. 189 (2019); Solon Barocas, Andrew D. Selbst & Manish Raghavan, *The Hidden Assumptions Behind Counterfactual Explanations and Principal Reasons*, PROCEEDINGS OF THE 2020 CONFERENCE ON FAIRNESS, ACCOUNTABILITY, AND TRANSPARENCY 80 (2020); Finale Doshi-Velez et al., *Accountability of AI Under the Law: The Role of Explanation* (Berkman Klein Ctr. for Internet & Soc'y, Working Paper, 2017); Andrés Páez, *The Pragmatic Turn in Explainable Artificial Intelligence (XAI)*, 29 MINDS & MACH.'S 441 (2019); Selbst & Barocas, *supra* note 4.

[61] In practice, Europe's adoption of the General Data Protection Regulation gives some legal bite to the concept of explainability. Margot Kaminski, *The GDPR's Version of Algorithmic Accountability*, JOTWELL: J. THINGS WE LIKE LOTS 1 (Aug. 16, 2018), https://cyber.jotwell.com/the-gdprs-version-of-algorithmic-accountability/ [https://perma.cc/5E9P-J27Y]; Kaminski, *supra* note 60.

[62] *See* Katherine J. Strandburg, *Rulemaking and Inscrutable Automated Decision Tools*, 119 COLUM. L. REV. 1851 (2019) at 1853–54 (noting this orientation); Kaminski, *supra* note 2 (same).

[63] Kaminski, *supra* note 2, at 1553.

[64] *See, e.g.*, Strandburg, *supra* note 62; Strandburg, *supra* note 60; Van Loo, *supra* note 7; Ryan Calo & Danielle Keats Citron, *The Automated Administrative State: A Crisis of Legitimacy*, 70 EMORY L. J. 797 (2021); Frank Pasquale, *A Rule of Persons, Not Machines: The Limits of Legal Automation*, 87 GEO. WASH. L. REV. 1 (2019).

[65] Nicholas Diakopoulos, *Algorithmic Accountability Reporting: On the Investigation of Black Boxes* (Tow Center for Digital Journalism, 2014) https://academiccommons.columbia.edu/doi/10.7916/D8ZK5TW2 [https://perma.cc/S4GN-YKQ4].

[66] Binns, *supra* note 2.

[67] Fung, *supra* note 54.

[68] VIRGINIA EUBANKS, AUTOMATING INEQUALITY 50-51 (2018).

[69] Rashinda Richardson et al., *Litigating Algorithms 2019 US Report* 20 (AI Now Inst. 2019).

[70] Bloch-Wehba, *supra* note 30, at 1277-78.

[71] *See* Kashmir Hill, *Wrongfully Accused by an Algorithm*, N.Y. TIMES: TECH. (June 24, 2020),

https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html [https://perma.cc/3UJE-TAEA]; Jay Greene, *Microsoft won't sell police its facial-recognition technology, following similar moves by Amazon and IBM*, Wash. Post, (June 11, 2020), https://www.washingtonpost.com/technology/2020/06/11/microsoft-facial-recognition/ [https://perma.cc/P37D-RNXS]; Ally Jarmanning, *Boston Bans Use Of Facial Recognition Technology. It's The 2nd-Largest City To Do So*, WBUR News (June 24, 2020), https://www.wbur.org/news/2020/06/23/boston-facial-recognition-ban [https://perma.cc/Q5BE-6XED]; Kyle Wiggers, *NYC passes POST Act, requiring police department to reveal surveillance technologies*, Venture Beat (June 18, 2020, 1:05 PM), https://venturebeat.com/2020/06/18/new-york-city-council-passes-law-requiring-nypd-to-reveal-its-surveillance-technologies/[https://perma.cc/5NDJ-U7DL].

[72] *See, e.g.*, Sandra G. Mayson, *Bias in, Bias out*, 128 Yale L. J. 2218 (2018–2019).

[73] Wexler, *supra* note 40; Ram, *supra* note 45.

[74] Elizabeth E. Joh, *The Undue Influence of Surveillance Technology Companies on Policing*, 92 N.Y.U. L. Rev. Online 101 (2017).

[75] Brennan Ctr. for Justice v. New York City Police Dept., 2017 N.Y. Misc. LEXIS 5138, at *9-10 (N.Y. Sup. Ct. Dec. 22, 2017).

[76] State v. Loomis, 881 N.W.2d 749 (Wis. 2016).

[77] Craig Timberg & Ellen Nakashima, *State Photo-ID Databases Become Troves for Police*, Wash. Post (Jun. 16, 2013), https://www.washingtonpost.com/business/technology/state-photo-id-databases-become-troves-for-police/2013/06/16/6f014bd4-ced5-11e2-8845-d970ccb04497_story.html [https://perma.cc/6PFN-V8F3].

[78] Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 Proc. of Mach. Learning Rsch. 15 (2018).

[79] Patrick Grother, Mei Ngan & Kayee Hanaoka, *Face recognition vendor test part 3: Demographic effects* (NIST Dec. 19, 2019).

[80] Mei Ngan & Patrick Grother, *Face Recognition Vendor Test (FRVT) - Performance of Automated Gender Classification Algorithms* (NIST Apr. 20, 2015); Buolamwini & Gebru, *supra* note 78).

[81] Sam Biddle, *Amazon's Ring Planned Neighborhood "Watch Lists" Built on Facial Recognition*, Intercept (Nov. 26, 2019, 2:53 PM), https://theintercept.com/2019/11/26/amazon-ring-home-security-facial-recognition/ [https://perma.cc/GV9A-4RBY]; Lauren Goode & Louise Matsakis, *Amazon Doubles Down on Ring Partnerships With Law Enforcement*, Wired (Jan. 7, 2020, 12:02 PM), https://www.wired.com/story/ces-2020-amazon-defends-ring-police-partnerships/ [https://perma.cc/7ZRN-FY85]; Dan Goodin, *Police use of Amazon's face-recognition service draws privacy warnings*, ArsTechnica (May 22, 2018, 7:00 PM), https://arstechnica.com/tech-policy/2018/05/police-use-of-amazons-face-recognition-service-draws-privacy-warnings/ [https://perma.cc/F7D8-X6S4]; Amrita Khalid, *Microsoft and Amazon are at the center of an ACLU lawsuit on facial recognition*, Quartz (Nov. 4, 2019), https://qz.com/1740570/aclu-lawsuit-targets-amazons-rekognition-and-microsofts-azure/[https://perma.cc/QH6Q-NFAR]; Caroline Haskins, *Amazon Requires Police to Shill Surveillance Cameras in Secret Agreement*, Vice (July 25, 2019, 11:54 AM), https://www.vice.com/en_us/article/mb88za/amazon-requires-police-to-shill-surveillance-cameras-in-secret-agreement [https://perma.cc/XQ6H-844C].

[82] Biddle, *supra* note 81; Drew Harwell, *Doorbell-camera firm Ring has partnered with 400 police forces, extending surveillance concerns*, Wash. Post: Tech. (Aug. 28, 2019, 6:53 PM), https://www.washingtonpost.com/technology/2019/08/28/doorbell-camera-firm-ring-has-partnered-with-police-forces-extending-surveillance-reach/ [https://perma.cc/5Q72-28LS].

[83] Biddle, *supra* note 81.

[84] Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, N.Y. Times: Tech. (Jan. 18, 2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html [https://perma.cc/Q2G6-H7FC].

[85] Ryan Mac, Caroline Haskins & Logal McDonald, *Clearview AI Says It Will No Longer Provide Facial Recognition To Private Companies*, Buzzfeed News (May 7, 2020), https://www.buzzfeednews.com/article/ryanmac/clearview-ai-no-facial-recognition-pri-

vate-companies [https://perma.cc/HJ8K-D2B4].

[86] Jay Greene, *Microsoft Won't Sell Police Its Facial-Recognition Technology, Following Similar Moves by Amazon and IBM*, WASH. POST (June 11, 2020, 2:30 PM), https://www.washingtonpost.com/technology/2020/06/11/microsoft-facial-recognition/ [https://perma.cc/4GS2-5SAZ].

[87] Simonson, *supra* note 6; Akbar, *supra* note 6; Allegra M. McLeod, *Prison Abolition and Grounded Justice*, UCLA L. REV. 1156 (2015); Dorothy E. Roberts, *Abolition Constitutionalism*, 133 HARV. L. REV. 1 (2019–2020); Roberts, *supra* note 6.

[88] I. Bennett Capers, *Race, Policing, and Technology*, 95 N.C. L. REV. 1241, 1273 (2016–2017) ("If we are going to watch some people, all of us should be watched.").

[89] Andrew Guthrie Ferguson, *The Exclusionary Rule in the Age of Blue Data*, 72 VAND. L. REV. 561 (2019).

[90] Capers, *supra* note 88, at 1276; *see also* Mayson, *supra* note 72; Aziz Z. Huq, *Racial Equity in Algorithmic Criminal Justice*, 68 DUKE L. J. 1043 (2019); Andrew D. Selbst, *Disparate Impact in Big Data Policing*, 52 GA. L. REV. 109 (2017–2018).

[91] Testimony of Marne Lenox before the New York City Council Committee on Public Safety, 3 (June 13, 2018) ("While the NYPD touts the declining number of police stops as evidence of its compliance with the law, the Department secretly continues to target, surveil, and catalog young men of color."), https://web.archive.org/web/20181009111929/http://www.naacpldf.org/files/case_issue/City%20Council%20Testimony%20combined%206.13.18.pdf; Sarah Brayne & Angèle Christin, *Technologies of Crime Prediction: The Reception of Algorithms in Policing and Criminal Courts*, SOC. PROBS. (2020), https://doi.org/10.1093/socpro/spaa004 [https://perma.cc/KE8W-CML6].

[92] *Cf.* Edwards & Veale, *supra* note 46.

[93] *Cf.* Frank Pasquale, *The Second Wave of Algorithmic Accountability*, L. & POL. ECON. PROJECT BLOG (Nov. 25, 2019), https://lpeblog.org/2019/11/25/the-second-wave-of-algorithmic-accountability/ [https://perma.cc/J3BJ-269F].

[94] Hannah Bloch-Wehba, *Democratic Algorithms* (2021) (Unpublished manuscript) (on file with author).

[95] *Cf.* Capers, *supra* note 88 at 1270 (describing expanded surveillance technology as "us[ing] the master's tools to tear down the master's house").

[96] Freeman, *supra* note 8 at 608–09 ("A contractual system of administration relies on judicial enforcement of private contract law at the behest of the supervising agency rather than judicial enforcement of administrative law principles at the behest of private citizens.").

[97] Mike Maharrey, *Nashville Metro Council Passes Ordinance Taking First Step Toward Limiting the Surveillance State*, TENTH AMENDMENT CTR. (June 13, 2017), https://blog.tenthamendmentcenter.com/2017/06/nashville-metro-council-passes-ordinance-taking-first-step-toward-limiting-the-surveillance-state/[https://perma.cc/EL8A-3Z3Q]; Mynorthwest Staff, *Seattle set to decide on the fate of 29 different surveillance technologies*, MY NW. (Oct. 24, 2018, 5:31 AM), https://mynorthwest.com/1156263/seattle-surveillance-ordinance-public-comment/? [https://perma.cc/U78N-JPZ8]; Jenna Fisher, *Cambridge Passes Law To Regulate Police Surveillance*, PATCH (Dec. 11, 2018, 4:46 PM), https://patch.com/massachusetts/cambridge/cambridge-passes-law-regulate-police-surveillance [https://perma.cc/CXP7-UF7S]; Eric Kurhi, *Pioneering spy-tech law adopted by Santa Clara County*, MERCURY NEWS (June 7, 2016, 10:35 AM), https://www.mercurynews.com/2016/06/07/pioneering-spy-tech-law-adopted-by-santa-clara-county/ [https://perma.cc/JKU5-V7LG].

[98] ACLU, *Community Control Over Police Surveillance (CCOPS) Model Bill* (ACLU Oct. 2020), https://www.aclu.org/other/community-control-over-police-surveillance-ccops-model-bill [https://perma.cc/4DFG-G6K5].

[99] *See* Ira S. Rubinstein, *Privacy Localism*, 93 WASH. L. REV. 1961 (2018) 2005–06 (documenting NYPD's objection to the Public Oversight of Surveillance Technology (POST) Act proposed in New York City).

[100] S. 6280, 66th Cong. (Wash. 2020), http://lawfilesext.leg.wa.gov/biennium/2019-20/Pdf/Bills/Senate%20Passed%20Legislature/6280-S.PL.pdf?q=20200601051554 [https://perma.cc/58Q7-YZTH].

[101] Dillon Reisman et al., *Algorithmic Impact Assessments: A Practical Framework for Public Agency Accountability* (AI Now Institute 2018), https://

ainowinstitute.org/aiareport2018.pdf [https://perma.cc/U6D9-UKFK].

[102] *See* Geoffrey H. Salomons & George Hoberg, *Setting boundaries of participation in environmental impact assessment*, 45 Env’t Impact Assessment Rev. 69 (2014); Heli Saarikoski, *Environmental impact assessment (EIA) as collaborative learning process*, 20 Env’t Impact Assessment Rev. 681 (2000) (articulating concerns about co-optation in environmental impact assessments, which have served as a model for algorithmic impact assessments).

[103] Bloch-Wehba, *supra* note 30.

[104] H.R. 4368, 116th Cong. (2019); H.B. 118, 2019 Leg., 65th Sess. (Idaho 2019); Crawford & Schultz, *supra* note 7, at 1945 n.18 (collecting other state and local initiatives).

[105] Rashida Richardson et al., *Confronting Black Boxes: A Shadow Report of the New York City Algorithmic Decision System Task Force* (AI Now Institute 2019), https://ainowinstitute.org/ads-shadowreport-2019.pdf [https://perma.cc/P6TG-TWDY].

[106] *Id.*

[107] OMB Memorandum M-16-21.

[108] *Id.*

[109] NIST, AI Standards, https://www.nist.gov/artificial-intelligence/ai-standards (“[M]any decisions still need to be made about whether there is yet enough scientific and technical basis to develop those standards provisions.”.)

[110] *Cf.* Pamela Samuelson & Kathryn Hashimoto, *Questioning Copyright in Standards*, 2 *in* The Cambridge Handbook of Technical Standardization Law: Further Intersections of Public and Private Law 91–107 (Jorge L. Contreras ed., 2019) (discussing copyright protection in standards).

[111] Office of Science and Technology Policy, Increasing Access to the Results of Federally Funded Scientific Research (Feb. 22, 2013), https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/ostp_public_access_memo_2013.pdf.

[112] Arvind Narayanan, *How to recognize AI snake oil* 21 (Princeton University) (2019) (https://www.cs.princeton.edu/~arvindn/talks/MIT-STS-AI-snakeoil.pdf [https://perma.cc/SD2Z-DYUW]).

[113] Miles Brundage et al., T*he Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*, ArXiv:1802.07228 (Feb. 20, 2018), http://arxiv.org/abs/1802.07228 [https://perma.cc/5AM7-WYJZ].

[114] Ida Sim et al., *Time for NIH to Lead on Data Sharing*, 367 Science 1308 (Mar. 2020).

[115] David Freeman Engstrom & Daniel E. Ho, *Algorithmic Accountability in the Administrative State*, 37 Yale J. on Regul. 800 (2020), https://digitalcommons.law.yale.edu/yjreg/vol37/iss3/1 [https://perma.cc/QDZ2-RH2Q].

[116] Meeri Haataja, Linda van de Fliert & Pasi Rautio, *Public AI Registers: Realising AI transparency and civic participation in government use of AI* 3 (Saidot Sept. 2020), https://uploads-ssl.webflow.com/5c8abedb10ed656ecfb65fd9/5f6f334b49d5444079726a79_AI%20Registers%20-%20White%20paper%201.0.pdf [https://perma.cc/8V6B-FKH2].

[117] *See, e.g.*, City of Helsinki AI Register, https://ai.hel.fi/en/ai-register/ [https://perma.cc/T49V-874H] (last visited Apr. 19, 2021); Algorithmic systems of Amsterdam, https://algoritmeregister.amsterdam.nl/en/ai-register/ [https://perma.cc/YL93-DNP5] (last visited Apr. 19, 2021).

[118] Draft Policies for Public Comment, https://www1.nyc.gov/site/nypd/about/about-nypd/public-comment.page [https://perma.cc/3PH6-SL6U] (last visited Apr. 19, 2021).

[119] Richardson, *supra* note 105.

[120] Bronwyn Howell, *Regulating artificial intelligence: Transparency and disclosure*, AEI (Jan. 4, 2019), https://www.aei.org/technology-and-innovation/innovation/regulating-artificial-intelligence-transparency-and-disclosure/. (“Information disclosure is one of the least intrusive forms of regulation (albeit that it is not always easy to monitor and enforce compliance).).”

[121] *See, e.g.*, Elizabeth Weill-Greenberg, *Chicago’s Gang Database Can Have “Devastating” Consequences, But There’s No Way To Be Removed From It*, Appeal (Dec. 18, 2019), https://theappeal.org/chicago-gang-database-lawsuit/ [https://perma.cc/7TS2-LMP2].

About the Author

Hannah Bloch-Wehba is an associate professor of Law at Texas A&M University School of Law who teaches and writes on law and technology. Her scholarship primarily focuses on free expression, privacy, and government accountability. Her interests include transparency and accountability for law enforcement, public access to information, and the use of new technologies in government decision making. She is also an affiliated fellow at Yale Law School's Information Society Project, an affiliated scholar at NYU School of Law's Policing Project, and a fellow at the Center for Democracy & Technology.

Acknowledgments

My thanks to Nicholas Brock, Bouquet Harger, and Jake Williams for essential research assistance and to David Haendler at Drexel University Kline School of Law's Legal Research Center for excellent research support. I am extremely grateful for comments from Jeff Bellin, Kiel Brennan-Marquez, Rebecca Crootof, David Greene, Jameel Jaffer, Amy Kapczynski, Zachary Kaufman, Christina Koningisor, Michael Mannheimer, Tim Mulvaney, Ngozi Okidegbe, Andrew Selbst, and Peter Yu that greatly improved this draft. My thanks to Ignacio Cofone and the student participants in the AI Regulation seminar at McGill Law. This paper would not have been completed in the absence of the generous feedback, support, and camaraderie of the Junior Law & Tech* Scholars Zoom Meetup of 2020.

About the Knight First Amendment Institute

The Knight First Amendment Institute at Columbia University defends the freedoms of speech and the press in the digital age through strategic litigation, research, and public education. It promotes a system of free expression that is open and inclusive, that broadens and elevates public discourse, and that fosters creativity, accountability, and effective self-government.

knightcolumbia.org

Design: Point Five
Illustration: ©Erik Carter

KNIGHT
FIRST AMENDMENT
INSTITUTE at
COLUMBIA UNIVERSITY