5

A Bouquet for Battling the Expansion of Trade Secrets in the Public Sector

Cynthia H. Conti-Cook

The best-designed bouquet may appear effortlessly assembled, but bouquets have their own understated architecture—a hearty focal-point flower, fillers for natural aesthetic, and several complimentary supporting flowers.[1] This chapter discusses how trade secrets in the public sector have been imported through new technologies, how they obstruct democracy and cause harm across many communities. It uses the bouquet—a floral arrangement—to illustrate its organization the way pillars or columns typically visualize the blueprint of written organizational structure. The sources gathered here, from the legal history of intellectual property to criminal court decisions to procurement processes to toolkits for organizers, do not always grow near one another or naturally cross-pollinate. Combined, they offer a strategic battle bouquet for organizers to protect the public from corporate control by targeting strategies aimed at the public purse.

This bouquet arrangement features five types of flowers. The focal-point flowers, the big show-stopping wide-open daisies, demand asymmetrical emphasis. Wide-open daisies hide nothing and center the public's right to know as a table-setting motivating principle and magnetized north star. These daisies are surrounded by baby's breath that lend a natural aesthetic—existing legal precedent evincing the historically persuasive logic of prioritizing the public's right to information. Roses are layered and overlapping social harms and bell-shaped wood hyacinths are the social movements already ringing the alarm bells. Finally, peonies are pain-relieving practical tools with which to intervene.

The organizing structure of the bouquet is central to the strategy it offers—to combat trade secrets in the public sector, we must organize ourselves around what we collectively need to know to protect each other and the future survival

of all living things. This chapter examines the patriarchal values driving trade secret battles by corporate entities that prioritize property over people, heavily invest in structures of secrecy, and protect dominant yet ahistorical narratives rather than governing through trust and consensus building by informed democratic participation.

By contrast, the healing peonies offered in this chapter prioritize people over property, embody collaborative relational strategies, center addressing harm, learning, and leadership from directly impacted people, and demand inclusive and joyful coalitions. Through the beautiful container of a bouquet, this chapter offers observations of already emerging strategies that address the confluence of state, corporate, and algorithmic secrecy—collaborative advocacy that fertilizes the soil of the public procurement process so that we all may better blossom.

DAISIES—THE PUBLIC'S NATURAL RIGHT TO INFORMATION

Before moving into how trade secrets obstruct access to information about technologies sold to the public sector, we shall set a hearty focal-point—a large wide-open daisy. Indigenous people around the world have long centered collaboration with Earth and all living things based on "a moral covenant of reciprocity [that] calls us to honor our responsibilities for all we have been given, for all that we have taken."[2] Biologist Rachel Carson similarly introduced this enduring reciprocity as a motivating principle in the first chapter of *Silent Spring*, "the classic that launched the environmental movement," with the following: "[the] public must decide whether it wishes to continue on the present road, and it can do so only when in full possession of the facts."[3] The public, *not* corporations, academics, experts, politicians, or billionaires, "*must* decide" how to balance survival with conditions needed to sustain future life. To execute this responsibility effectively, the public requires "full possession of the facts."[4] This principle is not limited to pollutants—it extends to all things potentially harming the public.

Carson grounded her principle not in legal or political history, but in natural rights philosophy.[5] The public's right to decide and be in full possession of the facts grows naturally from "our obligation to endure"—it is an evolutionary-driven natural right protecting our collective ability to sustain existence. Biologist Janine Benyus echoes this emphasis in her book *Biomimicry—Innovation Inspired by Nature*. One of the ten winning strategies she recommends we mimic, based on billions of years of evolution and across complex ecosystems, is to "run on information" and an abundance of feedback. "What makes a mature community run is not one universal message being broadcast from above, but numerous, even redundant, messages coming from the grass roots, dispersed throughout the community structure."[6] This flow of information will determine the sustainability of

our collective survival—"the *raison d'être* of mature communities, remember, is to maintain their identity throughout environmental storms and travails, so they can remain, and evolve, in place."[7]

Grounding this chapter in this natural right to information stemming from our "obligation to endure," and not corporate controlled information "broadcast from above," is both relevant to a discussion of trade secrets as well as strategic. Industrial drivers that invented intellectual property (IP) rights like trade secrets—and the courts that have adopted their arguments—have made the source of these rights relevant and central to justifying legal protections for information ownership.[8] Public demand for information is often successfully dismissed based on these dominant invocations of intellectual property, limiting the imaginative solution space to corporate self-audits,[9] protective orders,[10] and nondisclosure agreements.

Invoking natural rights also strategically anchors the conversation about trade secrets around the public's right to information. Hannah Bloch-Wehba called out critical technology scholars for "[neglecting] a critical avenue for promoting public accountability and transparency for automated decision-making: the law of access to government records and proceedings." Her work demonstrates how centering the public's right to know gives advocates a strategic legal advantage in fighting for algorithmic transparency.[11] Fortunately, there is also strong legal precedent for doing so.

BABY'S BREATH—EXISTING LEGAL PRECEDENT

The public's natural right to know is also supported by complimentary existing legal precedent, the baby's breath in this bouquet. Legal scholar Amy Kapczynski resurrected United States Supreme Court precedent "show[ing] that courts even at the height of laissez faire were clear about the *categorical priority of the public*, and rejected trade secret claims when they conflicted with the public's right to know"(emphasis added).[12] While we live in a world where technology companies are claiming everything from diversity policies to how they address gender-pay gaps would cause "competitive harm,"[13] Kapczynski revives a legal history that can shine on "the shadow of trade secret law."[14] We have before and can again subordinate corporate interests to the public good, aligned with the public's natural right to co-create its future through government.

When pressuring procurement systems around the consequences of contract terms, movements can cite this history to emphasize that the public is the primary stakeholder, not the corporate bottom line. Kapczynski asserts this as a "clear principle . . . [legislatures] and agencies have the right to disclose anything—even core trade secrets like product formulas—anytime they seek to reveal something relevant to consumers about the marketed product or service."[15] This is especially true in the context of new technologies. Advocates' attempts to reveal the extent

of preventable harms by public access requests simply seek information that the government using the technology has, the corporation has, but the person subjected to the technology often does not have access to. Optimistically, Kapczynski asserts that "together, these points indicate that Congress can condition [vendors'] market access on the turning over of trade secret data, and make that data public without working a takings, *at least if there is no express governmental promise before the submission of the data that [government] will refrain from doing this*."[16] The caveat, as mentioned earlier, is one we must pay attention to: when procurement officers and courts concede to corporate claims of confidentiality, it may unintentionally feed a factual corporate narrative that seeks to expand secrecy.

This trend is simply counterintuitive for a democracy, as David S. Levine presciently warned, "[if] we do nothing, [trade secrets] will be the infrastructure itself—owned and operated by private interests with commercial values like business advantage and secrecy of corporate information—that will direct the law involving public activity, rather than the law creating the conditions under which public infrastructure operates."[17] And as Bloch-Wehba said so well, the real obstacles to understanding technologies "are attributable, not to the sophistication of decision-making methodologies but to a more basic shift toward privatization and automation in government."[18] Increased secrecy is simply a feature, not a bug, of expanded neoliberalism.

ROSES—OVERLAPPING AND LAYERED HARMS

Intentionally documenting and articulating the overlapping and layered harms corporate secrecy introduces into the public sector must be done strategically and be led by people most deeply impacted. New technology researched and developed by private companies is bought by government agencies every day, from systems used for police investigation through electronic incarceration on parole supervision. It includes predictive policing, cell-site simulators, biometric tools, risk assessment tools, communications systems for detained people, and many more tools state actors use to surveil.[19]

Each of these technologies have context and technology-specific issues that contribute to its harms. Former public defender Vincent Southerland observed that "technology in the hands of law enforcement is a force multiplier"[20] and, therefore, also a harm multiplier.[21] Many tools in the hands of law enforcement cause various iterations of harm at varied degrees of severity—from potentially lethal and routinely abusive police interactions, to detention, family separation, deportation, and many more.[22] These layered harms and their solutions are best understood by those in immediate proximity to them. Those people tend to be disproportionately feminine, pregnant, Black, poor, disabled, migrating, or part of another historically oppressed community. Like layers of rose petals, these harms are occasionally obscured and overlapping, compounding suffering on those at the

intersections. Southerland describes how "[the] technologies erect digital borders around communities of color, fortifying the colony-in-a-nation status that defines those communities."[23] These conditions require arduous effort to organize against. Through legal constructs that promote secrecy, these efforts are often suppressed.

I have seen these efforts to organize thwarted firsthand. Around 2017, I represented a man incarcerated in New York who, along with two others, noticed discrepancies across the "COMPAS" scores relied on by the prison to evaluate eligibility for release.[24] This assessment is done by prison staff at a computer. My client introduced me to the two men, Glenn Rodriguez and Jose Piñeda, with whom he compared "risk" scores.[25] Mr. Rodriguez surveyed others and analyzed their risk scores to how staff used vast discretion to interpret a single subjective question.[26] Question 19 asked, "Does this person appear to have notable disciplinary issues?" How that specific question was answered, despite how vaguely it was written and how differently prison staff were interpreting it, determined whether it gave you a score of high ("yes"), medium ("unsure"), or low risk ("no").

Mr. Piñeda, whose counselor answered "unsure" for Question 19, made another observation—when the counselors were scrolling through the assessment, a bubble popped up above the question with additional instructions. He filed a Freedom of Information Law (FOIL) request with the prison for that language and for the training manual issued by COMPAS to train the state prison's counselors to try and understand what his counselor was "unsure" about—he only had two infractions in the last decade. The government responded that the information sought "are trade secrets or are submitted to an agency by a commercial enterprise or derived from information obtained from a commercial enterprise and which if disclosed would cause substantial injury to the competitive position of the subject enterprise."[27]

We sued to demand disclosure. The State argued that disclosure of the training manual "would cause substantial injury to the competitive position of this enterprise" despite failing to point to any evidence "or even a suggestion as to how the material requested" could be considered a trade secret.[28] The Court ruled in favor of a limited disclosure after a year of litigation. An officer brought the training manual to Mr. Piñeda's cell where he read what the bubble said: "Using all the information available to you and in your professional judgment did this person have significant disciplinary problems."[29] For Mr. Piñeda, the harms introduced by this risk assessment were layered. Forcing his mostly decades-old disciplinary history into a "yes, no, unsure" box and reducing his years of accomplishments into an estimated score dehumanized him in front of the parole board. After denied parole, his inability to access information that would help him correct the mischaracterization of his disciplinary history hampered his ability to appeal his denial and prevent the same thing from happening again.

More broadly, the obstruction meant that other people in prison could take only limited proactive action to protect their scores and push back on the use of

risk assessment's all together. The prison's deference to protecting the property interests of a company above the liberty interests of a person in prison fighting for parole release against an algorithm crystalizes how corporate secrecy creep manifests in the public sector.

This perversion of public sector values was even more explicit when a DNA software company appeared in an appellate criminal case out of California to fight against the accused's access to its calculations.[30] To support its claim for trade secrecy, the company offered what is likely a routine comparison in trade secret battles—its hours invested in the business.[31] Yet instead of competing against another business's number of hours, its adversary was a man facing fifty years in prison. Nevertheless, the company essentially argued "its property interests of 27,600 hours (or a little over three years) should weigh more than the hundreds of thousands of hours [the accused] potentially faces in prison, deprived of his liberty, freedom and family."[32] For a business to invest so much in a tool meant for criminal prosecutions without also expecting constitutional confrontation rights, like adversarial testing, to require disclosures demonstrates how problematically corporate claims to secrecy have eclipsed public protections in the procurement process.[33]

Some governments even agree explicitly to confidentiality terms in their contract.[34] As these trade secret cases emerged, they inspired a nascent research effort, joined by Jeanna Matthews and the NYU Technology Law and Policy clinic, to request law enforcement technology contracts across the country. We found contracts explicitly protecting the public's interest in accessing information—for example, in Allegheny County's Purchase Agreement with Cybergenetic—but we also found multiple contracts, like the Harris Corporation's contract in Chicago, that attempted to bind the state to confidentiality.[35] These confidentiality agreements do not, however, only hinder people seeking release after conviction from accessing information, like Mr. Piñeda. As Rebecca Wexler wrote, they also obstruct people accused of crimes from accessing and confronting evidence presented against them at trial. Public defenders are additionally generally underresourced to combat both prosecutors and corporate legal teams in trade secret battles, and when they do win access and find errors, faulty programs are rarely replaced.[36] When the systems are replaced,[37] the underlying government failures to filter for similar system errors in new programs still go unaddressed—simply put, litigation is not a viable strategy for preventing harm.[38]

In addition to the obstructions trade secrets introduce to a person's literal ability to fight for their freedom from incarceration, they also smuggle a more subtle danger into the public sector. Corporations in the future may try to point to government adoption of confidentiality terms and trade secret claims as factual precedent in attempts to limit public or even government access to aspects of their technologies.[39] While some court decisions allowing defense counsel more expansive access to materials under protective orders are celebrated for achieving

balance between competing interests, by consistently conceding the existence of trade secrets, courts feed corporate secrecy campaigns.[40] These fights will not be won in courts—we must follow movements now pointing at procurement.

WOOD HYACINTHS—MOVEMENTS RINGING ALARM BELLS

Social justice movements are responding to these harms by targeting local budgets and corporations, as well as organizing campaigns around aligning public funds with the public's interest. Wood-hyacinths are tiny flowers shaped like bells, and this section shines on a handful of movements already ringing alarm bells over corporate secrecy. Organizations like Worth Rises are creating tools to educate the public about corporate influence on government.[41] Advocates like Mijente, Surveillance Resistance Lab, and Just Futures Law are evolving their pressure campaigns to target shareholders and workers at specific corporations, like Equifax, that are sharing utility data with immigration enforcement.[42] Organizers are targeting contract cycles like election cycles[43] and mapping corporate capture like electoral maps.[44] Accessing information about these companies' contractual relationships to government is a crucial part of this work.

Media Justice, for example, hosts an interactive map about e-carceration, or electronic monitoring ("EM") companies. E-carceration companies in the United States alone operate app and ankle strap monitoring businesses worth hundreds of millions of dollars in government contracts for people before and after conviction.[45] "The average daily caseload of monitored individuals in . . . North America . . . amounted to about 282,000 . . . during 2020" and that number is projected to double by 2025, with additional "strong focus" projected for embedded software and analytics.[46]

Media Justice's Roadmap, "How to Build an Unshackling Freedom Campaign," targeting EM emphasizes "your starting point is information." It recommends that organizers, in addition to gathering stories from people subjected to e-carceration, understand the importance of "[accessing] as much official data on EM as you can" . . . "to effectively mobilize people to your campaign or challenge the talking points offered by proponents of EM."[47] Media Justice's own website marshals information about contracts, fees lobbed on those subjected to EM, taxpayers, and in some states, like Louisiana, they connect dots between judges ordering EM and company kickbacks.[48]

As EM companies incorporate more software and analytics into their devices, accessing information through public records requests may be increasingly obstructed by trade secret exemptions, as the prison attempted to do in Mr. Piñeda's case. Indeed, it is exactly this corporate entanglement that Media Justice's founder, Malkia Cyril, highlights as dangerous to the public's influence on the state: "e-carceration helps states become indebted to corporations and corporate

power."[49] Trade secrets, as currently tolerated by the public sector, serve to obscure the extent of this debt and power—they shroud corporate stakeholders invested in maintaining an expansion of carceral technology in secrecy.

PEONIES—PAIN-RELIEVING PRACTICAL TOOLS FOR PROCUREMENT INTERVENTIONS

The public procurement process is how government contracts for goods or services are established with private corporations and it can look different depending on whether it is federal, state, or local. The introduction of new technologies like risk assessment tools, surveillance systems, or any of the many other technologies and bundled services currently sold to governments requires a new procurement process—one that first interrogates the assumption that a data-driven tool will solve the problem presented and opens opportunities for public participation.

Procurement officers generally have the power to issue directives to its staff about what standards any new vendor or contract must meet. For example, for some specialized contracts, specific rules dictate how agencies can contract IT consulting services.[50] Similarly, procurement processes for technology vendors must introduce some threshold questions about what problem they are solving for—and invite public participation in that problem definition process early and often. Engaged public participation throughout the process of identifying a problem, understanding the scope of that problem, the potential for that problem to be addressed by a data-driven solution (or not) as well as the potential harms it introduces could better protect the public from harmful technologies. If public participation confirms that a technology solution would address the problem defined, additional opportunities for public input must arise to inform impact assessments, identify potential harms and mitigation strategies, consider a company's history, and identify metrics by which to measure the technology intervention's success. For now, these procurement processes are often opaque and difficult to pierce.

Fortunately, there are a handful of peonies—known for pain-relief—we can add to our bouquet. Rashida Richardson's *Guidance for Key Stages of Government Technology Procurement* can be used by advocates to support engagement with their local procurement officer. "This guidance offers high level considerations and recommendations that can improve transparency, accountability, oversight, and public trust in government technology procurement without legislative or regulatory reform."[51] Richardson identifies methods such as documenting pre-solicitation technology assessments, assessing solicitation approaches, proposal evaluation and contract negotiation, which procurement officers can use to better understand a technology—and the problem it seeks to solve. Similarly, Stephen Raher created a useful set of "Best Practices for Prison and Jail Tablet Procurement" through the Prison Policy Initiative applicable to many other digital contexts.[52] He identifies ways procurement of prison telecommunications services can

be "reinvented" by "[opening] up aspects of the procurement process to oversight" and "simply by modifying contracts or the terms of requests for proposals."[53] Catherine Crump also offers procurement "remedies to democratize local surveillance policy making" at federal, state, and local levels. Her suggestions include requiring involvement of elected representatives in technology procurement processes, requiring that technologies be governed by use policies, and additional state and local remedies.[54]

Elizabeth Joh also highlights public access laws as an important oversight mechanism.[55] An online resource, *Breaking the Lock: Accessing Public Records to Map Systems, Algorithms, and Data* specifically supports this strategy to help "activists, lawyers or anyone interested in filing an open records request to determine what to look and ask for in order to assess and potentially challenge government use of algorithmic systems."[56] For organizers working on corporate accountability campaigns, "Tech Inquiry" is a tool that can help uncover layers of intermediaries, subcontractors, and subsidiaries that make tracing a company's contracts challenging.[57] The website's creator, Jack Poulson, explains its importance: "[even] when investigating a single form of influence . . . the official government data sources (e.g., USASpending.gov) at best partially expose corporate hierarchies."[58] These are all tools that organizers can use to brainstorm research strategies, develop actionable toolkits, and build strategies targeting procurement of technology.

Too often, "[in] criminal justice software and in many other examples of black box decision-making software in areas like hiring or credit, the interests of those purchasing the software to make decisions can be very different than the interests of those being decided about."[59] Opening up the procurement process to more democratic engagement introduces the interests of "those being decided about" in both defining the problem, evaluating whether the technology solution is responsive or potentially introducing new harm that weighs against its use, or requires impact assessments or other harm mitigation efforts.

Through multiple strategies including research, pressure campaigns on procurement officers, corporate accountability campaigns, public record litigation, communications strategies, and more, advocates can begin to push for more public interest values by pulling at purse strings.[60]

A BOW TO TIE IT ALL TOGETHER—IN CONCLUSION

Silent Spring's last chapter was "The Other Road."[61] Carson writes "[the] other fork of the road—the one "less traveled by"—offers "our last, our only chance to reach a destination that assures the preservation of our earth."[62] For the same reasons that Carson argued the insecticide industry cannot shape climate policy, we must also not allow states and corporations to govern us through a triple threat of police, corporate, and algorithmic secrecy that prioritizes corporate wealth above the public's right to co-create its future.

Protecting our right to information through interventions with the procurement process will become increasingly important harm management given future battles over data ownership, the inextricable connection between bodily and digital autonomy,[63] and the increased production of data-extraction tools set in communal infrastructures (i.e., "smart" cities). As Kapczynski explained, "trade secret law, because it protects only commercially valuable information that has been kept secret, neatly excludes ordinary people as 'owners' of data produced by or about them—even as it has expanded to incorporate an almost limitless amount of business data."[64] The expansion of technologies and trade secrets into the public sector combined with the toxic appetite companies have for claiming all data is their trade secret leaves little room left for democracy.

To imagine beyond harm mitigation strategies, if we were to let ourselves be led by Indigenous people's governance and agricultural practices, take Carson's "other road" or perhaps be the bouquet thrown by Banksy's *Rage, the Flower Thrower* into futures we define, how would the world look?[65] If the public's right to know dominated as a motivating principle over corporate financial interests and power, as the Supreme Court previously said it should, how might organizers, wise to the dangers of corporate capture of the state, recreate public procurement policies to ensure vendors capitulate to the public's demand for "full possession of the facts"? Perhaps we would prohibit privatized public sector technology contractors in the first place and return such services to more accountable government agencies and entirely rethink the privatization of punishment, or state-sanctioned punishment itself.

Rooting ourselves back into our collective right to be in full possession of the facts—stemming naturally from "our obligation to endure"—perhaps also leads to a place without prisons, private vendors, or bow-tied bouquets. Flowers remain rooted in the ground, growing wild; they are never overplanted with pesticides, picked by underpaid people, separated, or sold. A place where public procurement prioritizes principles of permaculture in government services—care for Earth, care for people—and protect the public's right to know what it needs to know in order to collectively endure.[66]

NOTES

Cynthia Conti-Cook extends many blue hydrangeas of gratitude for thoughtful feedback and encouragement to her former Legal Aid Society colleagues Terri Rosenblatt, Rebecca Wexler, Jessica Goldthwaite, Jerome Greco, as well as Glenn Rodriguez, Jose Piñeda, Vincent Southerland, Jeanna Matthews, Dana Delger, Michelle Shevin, and Paromita Shah. My gratitude also goes to the many inspiring people and organizations whose lived experiences, organizing, writing, and research is described within—flowers to all of you for striving to make this world more beautiful by being here. And to the late Chris Kuhlman, my hometown florist who taught me that flowers have their own language, a bushel of forget-me-nots for consulting with me on this bouquet last year. Rest well under the shade of big, beautiful petals.

1. *How to Make a Floral Bouquet in 6 Simple Steps*, MasterClass (June 7, 2021), https://www.masterclass.com/articles/how-to-make-a-bouquet#3-tips-for-picking-flowers-for-a-bouquet.

2. Robin Wall Kimmerer, Braiding Sweetgrass—Indigenous Wisdom, Scientific Knowledge, and the Teachings of Plants, 384 (2013).

3. Rachel Carson, Silent Spring, 13 (1962).

4. Not all facts are helpful to this end—overwhelming data dumps that drown out important information, for example, are not helpful.

5. Carson, *supra* note 3 (quoting natural philosopher Jean Rostrand).

6. Janine Benyus, Biomimicry: Innovation Inspired by Nature, 274 (1997).

7. *Id*.

8. Letter from A. R. Wallace to Charles Darwin, n.5 (July 2, 1866), *in* Darwin Correspondence Project, https://www.darwinproject.ac.uk/letter/DCP-LETT-5140.xml#back-mark-5140.f5 (industrialist Herbert Spencer, pointing to Charles Darwin's research, coined the phrase "survival of the fittest").

9. Central Digital & Data Office, *Data Ethics Framework*, GOV.UK (Sept. 16, 2020), https://www.gov.uk/government/publications/data-ethics-framework/data-ethics-framework-2020#specific-actions.

10. Rebecca Wexler, *Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System*, 70 Stan. L. Rev. 1343, 1418 (2018).

11. Hannah Bloch-Wehba, *Access to Algorithms*, 88 Fordham L. Rev. 1265 (2020).

12. Amy Kapczynski, *The Public History of Trade Secrets*, 55 U.C. Davis L. Rev. 1367, 1367 (2022).

13. Julienne Pepitone, *Black, Female, and a Silicon Valley "Trade Secret,"* CNN (Mar. 17, 2013, 8:00 AM), https://www.cnn.com/2013/03/17/us/black-female-and-a-silicon-valley-trade-secret/index.html.

14. Kapczynski, *supra* note 12, at 1428.

15. *Id*., at 1440.

16. *Id*., at 1418.

17. David S. Levine, *Secrecy and Unaccountability: Trade Secrets in Our Public Infrastructure*, 59 Fla. L. Rev. 136, 140 (2007).

18. Bloch-Wehba, *supra* note 11, at 1270–71.

19. *See id*., at 1273–86 (a more exhaustive list).

20. Vincent Southerland, *The Master's Tools and a Mission: Using Community Control and Oversight Laws to Resist and Abolish Police Surveillance Technologies*, 70 UCLA L. Rev. (June 16, 2023).

21. *Id*., at 15–18.

22. Aaron Sankin, Dhruv Mehrotra, Surya Mattu & Annie Gilbertson, *Crime Prediction Software Promised to Be Free of Biases. New Data Shows It Perpetuates Them*, The MarkUp (Dec. 2, 2021, 8:00 ET), https://themarkup.org/prediction-bias/2021/12/02/crime-prediction-software-promised-to-be-free-of-biases-new-data-shows-it-perpetuates-them.

23. Southerland, *supra* note 20, at 19.

24. N.Y. State Dep't of Corrs. and Cmty. Supervision, COMPAS Assessments/Case Plan (Aug. 14, 2019), https://doccs.ny.gov/system/files/documents/2020/11/8500.pdf ("COMPAS" stands for "Correctional Offender Management Profiling for Alternative Sanctions"); *see also* Julia Angwin, Jeff Larson, Surya Mattu & Lauren Kirchner, *Machine Bias*, ProPublica (May 23, 2016), https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

25. Both Mr. Rodriguez and Mr. Piñeda consented to their stories being shared in this chapter.

26. Rebecca Wexler, *Code of Silence*, Washington Monthly (June 11, 2017), https://washingtonmonthly.com/2017/06/11/code-of-silence/; *see also* Wexler, *supra* note 10, at 1370. Mr. Rodriguez presented his research in multiple venues. Brookings Institution, *Forensic Algorithms: The Future of Technology in the US Legal System* at 22:29, YouTube (May 12, 2022), https://www.youtube.com/watch?v=YNFEdElUT-4. Mr. Rodriguez and myself also presented his research and its implications. Ass'n for Computing Mach., *2019 Implications Tutorial: Parole Denied: One Man's Fight against a COMPAS Risk Assessment*, YouTube (Feb. 22, 2019), https://www.youtube.com/watch?v=UySPgihj70E.

27. N.Y. Pub. Off. Law § 87 (McKinney 2022).

28. Jose Piñeda, N.Y. State Dept. of Corrs. and Cmty Supervision, No. 903104–19, 10 (Oct. 11, 2019).

29. As documented in correspondence from Mr. Piñeda, in possession of author.

30. The type of software system in question was a probabilistic genotyping system (or PG system). Marc Canellas describes PG systems in Defending IEEE Software Standards in Federal Criminal Court as "heuristically developed forensic science driven by law enforcement goals, not science. It uses Markov chain, Monte Carlo methods that purportedly enable the identification of individuals from tiny samples of DNA that contain a mix of people's genetic material." Marc Canellas, *Defending IEEE Software Standards in Federal Criminal Court*, Computer (June 7, 2021), at 15.

31. People v. Superior Court (Dominguez), 28 Cal. App. 5th 223 (ESR brief filed 05/10/2018 at 3) (2018). People v. Superior Court (Dominguez), 28 Cal. App. 5th 223, at 227 (2018). The procedural history was summarized by the court—"Dominguez was initially tried in 2011; that jury hung. Upon his subsequent retrial, he was convicted of first-degree murder (Pen. Code, § 187, subd. [a]) and conspiracy to commit murder (id. §§ 182, subd. [a][1], 187). We upheld that conviction in People v. Dominguez (July 5, 2013, D060019) [nonpub. Opn.]). In 2017, the superior court granted Dominguez's petition for writ of habeas corpus, reversing his conviction." *Id.*, at 227 n.1. He had previously been serving a fifty-year sentence on the same charge. Greg Moran, *Murder Case That Highlighted DNA-Analysis Controversy Ends with Plea to Reduced Charge, Release*, San Diego Union-Tribune (Dec. 6, 2019), https://www.sandiegouniontribune.com/news/courts/story/2019-12-06/murder-case-that-highlighted-dna-analysis-controversy-ends-with-plea-to-reduced-charge-release.

32. Brief for the Legal Aid Society as amicus curie at 28, People v. Superior Court, 28 Cal. App. 5th 223 (2018)(filed 07/05/18) (I co-authored this brief with Legal Aid colleagues).

33. See Wexler, *supra* note 10.

34. Stingray Equipment Under GSA Contract *(# GS-35F0283J, § 4.5); See also* Tim Cushing, *Harris Stingray Nondisclosure Agreement Forbids Cops from Telling Legislators*, Techdirt (Jan. 25, 2018), https://www.techdirt.com/2018/01/25/harris-stingray-nondisclosure-agreement-forbids-cops-telling-legislators-about-surveillance-tech/.

35. *Allegheny County's Purchase Agreement with Cybergenetics (Purchase Agreement* #73948, *§ 10.2)* (Feb. 19, 2009).

36. Rachel B. Warren & Niloufar Salehi, *Trial by File Formats: Exploring Public Defenders' Challenges Working with Novel Surveillance Data*, Pros. of the Ass'n for Computing Mach. on Human-Computer Interaction (Apr. 2022), https://dl.acm.org/doi/pdf/10.1145/3512914.

37. By the time ProPublica won access to a tool developed by the Office of Medical Examiners in New York City, the agency already procured a vendor to replace it. Lauren Kirchner, *Federal Judge Unseals New York Crime Lab's Software for Analyzing DNA Evidence*, ProPublica (Oct. 20, 2017), https://www.propublica.org/article/federal-judge-unseals-new-york-crime-labs-software-for-analyzing-dna-evidence.

38. "If, in 5–10 years, defense attorneys are alone and still fighting over access to source code . . . we will have failed." Marc Canellas, Att'y, Off. of the Pub. Def., Cnty. of Arlington & the City of Falls Church, Engineers v. PGS: A Strategy for the War against Carceral Technology at the Legal Aid Society's DNA Unit's Foundation of DNA Defense: Unpacking the 2021 NIST Report (Apr. 1, 2022).

39. Kapczynski, *supra* note 12, at 1418.

40. *See State v. Pickett*, 466 N.J. Super. 270 (N.J. Super. Ct. App. 2021).

41. *The Prison Industry: Mapping Private Sector Players*. Worth Rises (Apr. 2020), https://worthrises.org/theprisonindustry2020.

42. Drew Harwell, *Utility Giants Agree to No Longer Allow Sensitive Records to Be Shared with ICE*, Washington Post (Dec. 8, 2021), https://www.washingtonpost.com/technology/2021/12/08/utility-data-government-tracking/.

43. Fran Spielman, *ShotSpotter Contract Comes Under Heavy Fire*. Chicago Sun-Times (Nov. 12, 2021), https://chicago.suntimes.com/city-hall/2021/11/12/22778971/shotspotter-contract-police-districts-city-council-gunfire-violence-crime.

44. *Electronic Monitoring Hotspot Map*, Media Justice (2022), https://mediajustice.org/electronic-monitoring-hotspots/; Nat'l Immigration Project, Immigrant Def. Project & Mijente, *Who's Behind ICE: the Tech Companies Fueling Deportations*, Mijente (Oct. 23, 2018), https://mijente.net/wp-content/uploads/2018/10/WHO%E2%80%99S-BEHIND-ICE_-The-Tech-and-Data-Companies-Fueling-Deportations-_v1.pdf.

45. *Electronic Offender Monitoring Solutions Market Trends and Drivers 2021: Stronger Focus on Software and Analytics within Offender Monitoring*—ResearchAndMarkets.com, Business Wire (Dec. 14, 2021), https://www.businesswire.com/news/home/20211214005999/en/Electronic-Offender-Monitoring-Solutions-Market-Trends-and-Drivers-2021-Stronger-Focus-On-Software-and-Analytics-Within-Offender-Monitoring.

46. *Electronic Offender Monitoring Solutions—2nd Edition*, ResearchAndMarkets (Dec. 14, 2021), https://www.researchandmarkets.com/reports/5509412/electronic-offender-monitoring-solutions-2nd#src-pos-1.

47. *Unshackling Freedom Toolkit*, MediaJustice, https://mediajustice.org/unshackling-freedom/what-you-can-do/ (accessed Apr. 3, 2023).

48. *Electronic Monitoring Hotspot Map: Louisiana*, MediaJustice, https://mediajustice.org/electronic-monitoring-hotspots/louisiana/ (accessed Apr. 3, 2023).

49. MediaJustice, *Understanding E-Carceration: A Community Event on the Future of Surveillance & Mass Incarceration* at 10:19, YouTube (Mar. 23, 2022), https://www.youtube.com/watch?v=nwZIUqTma04.

50. The City of New York Office of the Comptroller, *Internal Control and Accountability Directives: Directive #31: Special Audit Procedures for Information Technology Consulting and Other Information Technology Professional Services Payment Requests under Contracts Specifying Payment to a Vendor Based on Time* (July 1, 2014), https://comptroller.nyc.gov/wp-content/uploads/documents/Directive-31-Special-Audit-Procedures-for-IT-Consulting-etc.-Reformatted.pdf.

51. Rashida Richardson, *Best Practices for Government Procurement of Data Driven Technologies: A Short Guidance for Key Stages of Government Technology Procurement*, Ctr. for L., Info., and Creativity (May 2021), https://riipl.rutgers.edu/files/2021/05/Best-Practices-for-Government-Technology-Procurement-May-2021.pdf. Richardson adds parenthetically "(though modernization of procurement laws and policies is highly encouraged").

52. Stephen Raher, *Best Practices for Prison and Jail Tablet Procurement*, Prison Policy Initiative (July 14, 2022), https://www.prisonpolicy.org/messaging/rfp_guidance.html.

53. Stephen Raher, *The Company Store and the Literally Captive Market: Consumer Law in Prisons and Jails*, 17 Hastings Race & Poverty L.J. 3, 77 (2020).

54. Catherine Crump, *Surveillance Policy Making by Procurement*, 91 Wash. L. Rev. 1595, 1655–60 (2016).

55. Elizabeth E. Joh, *The Undue Influence of Surveillance Technology Companies on Policing*, 91 N.Y.U. L. Rev. Online 101, 125 (2017).

56. Rashida Richardson, Amba Bak & Ian Head. *Breaking the Lock: Accessing Public Records to Map Systems, Algorithms and Data*, FOIA Basics for Activists (Mar. 2022). https://www.foiabasics.org/breaking-the-lock.

57. Tech Inquiry, https://techinquiry.org/ (accessed Apr. 3, 2023).

58. Jack Poulson, *Easy as PAI (Publicly Available Information)*, Tech Inquiry 1–2 (Sept. 10, 2021), https://techinquiry.org/EasyAsPAI/resources/EasyAsPAI.pdf.

59. Jeanna Matthews, et al., *When Trusted Black Boxes Don't Agree: Incentivizing Iterative Improvement and Accountability in Critical Software Systems, in* AIES' 20: Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society, 13 (2020).

60. For example, Boston, MA, centered its constituents in technology procurement in this playbook. Mayor's Office of New Urban Mechanics, Boston Smart City Playbook, https://monum.github.io/playbook/#play6 (accessed Apr. 3, 2023).

61. Carson, *supra* note 3, at 277.

62. *Id*.

63. Rebecca Chowdhury, *America's High-Tech Surveillance Could Track Abortion-Seekers, Too, Activists Warn*, Time (June 6, 2022), https://time.com/6184111/abortion-surveillance-tech-tracking/.

64. Kapczynski, *supra* note 12, at 1442.

65. "Rage, the Flower Thrower" by Banksy was the subject of a famous trademark battle. Anny Shaw, *Banksy Loses Trademark Battle over His Famous Flower Thrower*, The Art Newspaper (Sept. 17, 2020), https://www.theartnewspaper.com/2020/09/17/banksy-loses-trademark-battle-over-his-famous-flower-thrower-image.

66. *How to Start a Permaculture Garden*, MasterClass (June 7, 2021), https://www.masterclass.com/articles/how-to-start-a-permaculture-garden#what-is-permaculture.