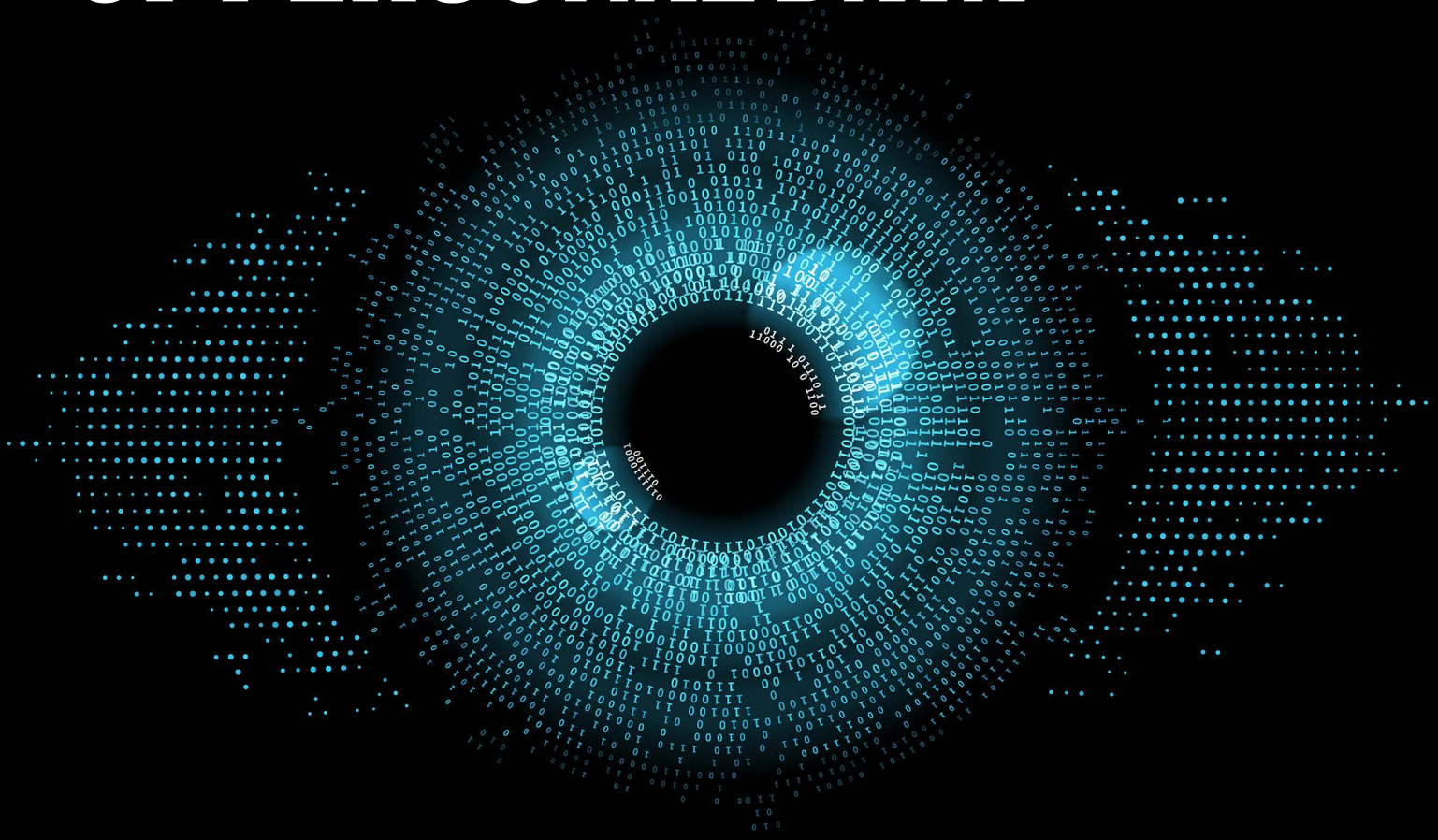
THE CENTER ON RACE INEQUALITY & THE LAW
NYU SCHOOL OF LAW

The Forensic Evidence Table

FORENSIC DEFENSE CLINIC

THE DATA JUSTICE ACT: REINING IN THE STATE'S COLLECTION AND USE OF PERSONAL DATA



BY DANIELLE RESHEFF, RACHEL WITT, MANEKA SINHA, ELIZABETH DANIEL VASQUEZ, NINA LOSHKAJIAN & VINCENT SOUTHERLAND

CONTENTS

CITE AS:

Cite as: Danielle Resheff, Rachel Witt, Maneka Sinha, Elizabeth Daniel Vasquez, Nina Loshkajian & Vincent Southerland, The Data Justice Act: Reining In the State's Collection and Use of Personal Data (2026), www.law.nyu.edu/documents/data-justice-act.

KEY TAKEAWAYS

This report critically examines the state's now-pervasive collection and use of personal data and, in response, introduces the Data Justice Act (DJA). Together, this report and the DJA articulate core principles grounded in two basic premises: personal data belongs to the individual, and the state's use of such data must be narrow, lawful, transparent, and accountable.

These core principles establish: (1) rights and values protecting individuals and their data; (2) safeguards requiring necessity, proportionality, and independent oversight of state data collection and use; (3) limitations on retention and secondary data use; and (4) enforceable procedural rights and remedies.

Their aim, in part, is to ensure that individuals can challenge unlawful collection, contest algorithmic deficiencies, and obtain redress when data is misused. These principles articulate a new vision of personal data not as information the state may freely access, but as something inherently ours, subject only to narrow intrusion. Leveraging these principles, the DJA aims to rein in the state's uninhibited control over our personal data.

KEY TAKEAWAYS

HARMS

1.
Modern surveillance systems undermine core civil liberties and democratic values.

2.
Unregulated data systems inflict concrete harms in the criminal context, including the escalation of police contact, the erosion of due process, and the imposition of life-altering penalties.

3.
Surveillance technologies disproportionately target and burden marginalized communities.

4.
Without upstream limits on data collection, the surveillance ecosystem remains an unchecked threat to fundamental rights and values.

RIGHTS AND VALUES

5.
The modern right to privacy is robust. Individuals are protected from persistent surveillance, retain the right to be let alone, and have the right to be forgotten once lawful use of data concludes.

6.
Individuals must receive clear, timely notice of data collection and be able to give or revoke valid, informed consent.

7.
Surveillance practices must not disproportionately target or burden marginalized communities.

8.
No one should face legal consequences based on automated tools without the ability to contest algorithmic decision-making.

9.
Personal data is, at the very minimum, an individual's property; the state cannot seize, retain, or repurpose it without lawful authority.

LIMITATIONS ON STATE USE OF DATA

10.
State actors cannot indefinitely retain or use personal data for unauthorized purposes.

11.
In criminal proceedings, state actors must disclose all data collected or used, and held by public or private entities, to accused persons and courts.

SAFEGUARDS

12.
Data collection must meet standards of necessity, specificity, and proportionality.

13.
Data access records must be logged, transparent, and accessible.

14.
Oversight bodies regulating state data collection and use must be empowered with genuine authority.

15.
Algorithmic tools used for data analysis must be transparent and explainable.

PROCEDURAL RIGHTS AND REMEDIES

16.
Individuals must be able to challenge algorithmic logic, error rates, and hidden biases.

17.
Individuals must have enforceable procedural rights to challenge data collection and use.

18.
Individuals must have enforceable remedies, including a private right of action, collective redress, exclusion of unlawfully obtained evidence, and automatic deletion of data after lawful use concludes.

"BIG BROTHER IS WATCHING YOU."[1]

In 1949, when George Orwell's dystopian classic *Nineteen Eighty-Four* was first published, the idea of our government having the capacity to constantly surveil us may have seemed fantastical. But, in the decades since, Orwell's imagined telescreens have evolved from fiction to reality: they are our phones, our cameras, our search histories, our walks to work, our social media activity, and nearly every other aspect of our daily lives. Without realizing it, we constantly hand the state a detailed map of our everyday activities. Each swipe of a public transit card logs our location and movement through the city. License plate readers track our cars block by block. Cell towers, traffic cameras, and public Wi-Fi networks silently record where we go and when.

Yet, as scholars note, Orwell's metaphor only captures part of the problem. Privacy scholar Daniel Solove cautions that modern surveillance is not overt and oppressive in the Orwellian sense but rather "sparkles." Modern data collection and use is hidden within everyday conveniences, generating harms more akin to an opaque bureaucracy than "Big Brother's" visible eye.[2] Professor Virginia Eubanks similarly warns that "Big Brother is not watching you, he's watching *us*."[3] The state monitors not only individuals but also social groups.[4]

INTRODUCTION

Little in modern life is as wholly unregulated as the state's collection and use of personal data. Today, state agencies have access to an ever-growing arsenal of powerful digital surveillance tools that enable tracking, monitoring, and databasing at a scale once unimaginable. Even our bodies are datafied.[5] Devices like period or sleep trackers turn our physiology into data, creating intimate new ways for the state to surveil us. Modern life has created a powerful infrastructure for state observation.

Data collected for benign or administrative reasons can be repurposed when political conditions change. After *Dobbs v. Jackson Women's Health Organization*,[6] public concern focused on whether period-tracking and fertility apps could be turned against their own users.[7] Leading scholars in this area, Professors Barry Friedman and Danielle Citron, note that these fears were justified because law enforcement has already sought personal data to investigate reproductive decisions.[8] They explain that reproductive health apps became a symbol of a broader structural problem: at scale, even mundane data points become intimate insights that can be retrieved, reconstructed, and weaponized long after a person believed they had done nothing wrong.[9]

Despite the vast power that datafication gives the state over civilians, the state's ability to collect and use personal data has grown unchecked by legislatures, courts, and the public. The danger lies not just in exposure, but in the unseen systems of data collection, analysis, and control that shape what governments know about us and how they can use that information.[10] The aggregation, storage, and secondary use of personal data covertly shifts the balance of power between individuals and the state.

While federal and state law provide some protections for personal data, these frameworks are piecemeal and limited in scope. The Stored Communications Act, for example, only covers wired or electronic communications in electronic storage.[11] Other state-level statutes, like the Illinois Biometric Information Privacy Act, protect specific data types but leave significant gaps in regulation of broader collection, secondary use, and aggregation of data.[12] The *Data Justice Act* (DJA) synthesizes these efforts and articulates a comprehensive framework that recognizes a new vision of personal data: not as information the state may freely access, but as something inherently *ours*, subject only to narrow intrusion, bridging gaps left by existing laws.

Surveillance technologies and the datasets that they produce erode people's basic civil rights and liberties. In New York, for example, a teenager living in a particular public housing complex might be added to the New York City Police Department's (NYPD) gang database just for adding certain hashtags to a social media post.[13] Even without any suspicion of criminal activity, young people in these communities may have their online presence monitored by the NYPD's Social Media Analysis & Research Team or be approached by undercover officers posing as peers.[14] Once labeled as gang members, they face heightened surveillance: frequent police stops, aggressive questioning about their peers and community, and the risk of having their phones seized.[15] In Chicago, federal agents relied on internal Department of Homeland Security identifiers that treat Chicago Bulls hats and Michael Jordan apparel as gang markers.[16] One Maryland father was detained and deported after police paperwork cited his Chicago Bulls hat and sweatshirt as gang indicators and referenced a disputed anonymous tip, before the Supreme Court ruled that such detainees must have a chance to challenge their removal.[17] These practices transform ordinary participation in daily life into a conduit for constant state surveillance and monitoring, embedding structural discrimination into the very architecture of the relationship between citizens and the state.

THE DJA CENTERS INDIVIDUAL RIGHTS AND DEMOCRATIC VALUES, SETS CLEAR LIMITS ON STATE DATA USE, AND ESTABLISHES ROBUST PROCEDURAL SAFEGUARDS. IT ALSO RECOGNIZES PERSONAL DATA AS A FORM OF PROPERTY BELONGING TO INDIVIDUALS, NOT THE STATE, THAT CANNOT BE INDEFINITELY RETAINED, REPURPOSED, OR COMMODIFIED.

Left unchecked, surveillance practices chill free expression and association, undermine the constitutional promise of equal protection, and erode the zone of autonomy necessary for a functioning democracy. State and local law enforcement agencies have repeatedly monitored political activists, demonstrators, and social media users without individualized suspicion or meaningful transparency. The American Civil Liberties Union has documented years of "illegal and unnecessary spying" on peaceful protesters, including anti-war, animal rights, and racial justice movements.[18] In Washington, D.C., the Brennan Center for Justice obtained over 700,000 pages of records showing that the

Metropolitan Police Department tracked social media posts about racial justice protests.[19] These practices may appear to be routine investigative techniques, yet they can discourage individuals from participating fully in civic life.

For communities that have historically borne the brunt of policing and law enforcement, surveillance technologies only exacerbate injustice.[20] Automated systems generate inequitable outcomes.[21] Tools like facial recognition software, predictive policing technology, and DNA databases disproportionately target Black, Latine, Indigenous, and other marginalized communities, entrenching longstanding patterns of discrimination and eroding public trust.[22] Police reliance on technologies like these routinely results in wrongful arrests and convictions and police violence.[23]

The modern data economy operates through practices of extraction and control that closely parallel historic systems of exploitation. Professor Chaz Arnett explains that just as cotton once fueled American industrial growth through the forced labor of enslaved people, data now serves as the raw material of the digital economy, with its value extracted from the capture and monetization of human lives and behaviors.[24] Understood through this lens, the harms of state surveillance are not merely technological but structural, rooted in the same racial and economic logics that once justified slavery and now sustain digital inequity.[25]

This report introduces the DJA, attached in the Appendix, model legislation that provides a framework to confront the growing threats posed by the state's collection and use of personal data. The DJA centers individual rights and democratic values, sets clear limits on state data use, and establishes robust procedural safeguards. It also recognizes personal data as a form of property belonging to individuals, not the state, that cannot be indefinitely retained, repurposed, or commodified. The DJA seeks to reinforce constitutional rights and widely held privacy values while filling the gaps that have left modern surveillance largely unregulated. It articulates a vision of personal data as a matter of ownership and autonomy rather than a resource for unchecked state power.

The DJA's core principles, as detailed below in *Legislative Aims*, are grounded in established constitutional and democratic rights and values, including:

- First Amendment values of free expression and association;
- Fourth Amendment protections against unreasonable searches and seizures, such as individualized suspicion, tailored collection, and judicial oversight;
- Fourteenth Amendment values of notice, due process, and equal protection; and
- Common law property rights.

The DJA proceeds from an acknowledgment that while the Constitution safeguards some of our rights, its protections are insufficient in the face of modern surveillance and data exploitation, requiring targeted legislative action. We have been cautioned that modern surveillance technologies create "intimate window[s]" into people's lives,[26] yet courts and legislatures have struggled to comprehensively regulate their use. While "the right to be let alone" has been recognized by many as a core American democratic value,[27] courts and scholars alike have struggled to define the scope and limits of its constitutional protection. Community organizers, legal scholars, and legislators have therefore repeatedly called for statutory safeguards to fill the gaps left by the Constitution with respect to government collection and use of personal data.[28] The DJA translates constitutional principles and democratic values into enforceable statutory protections capable of meeting the challenges of the digital age.

Existing federal efforts to define data privacy rights illustrate why such safeguards are needed. Although the Privacy Act of 1974 was enacted to constrain government actors, its broad law-enforcement exemptions allow agencies to remove entire systems of records from the Act's accuracy, purpose-limitation, and transparency requirements, a gap Congress expected to address through later legislation that never materialized.[29]

We recognize that jurisdiction-specific political realities may limit how the DJA can be implemented in practice. The DJA and this report, accordingly, are intended to serve as a framework and point of reference, not a rigid prescription. Jurisdictions and policymakers may adapt, modify, or selectively apply its provisions as appropriate to their particular legal and political contexts.

HARMS

THREATS TO CIVIL LIBERTIES AND DEMOCRATIC VALUES

Our personal data paints a detailed portrait of our lives, one which may seem innocuous in isolation but can quickly become damaging to our livelihoods, freedoms, and dignity when accessed by state actors. When aggregated and accessible to the state, such information can lead to mischaracterizations, stigma, and unwarranted surveillance of individuals and communities. The harms of surveillance are therefore not abstract: they are immediate, concrete, and often irreversible.

Even when surveillance tools function as intended, they pose profound civil liberties concerns. Reliable technologies create infrastructure for persistent monitoring, expanding the state's ability to observe and track individuals with unprecedented ease. Such systems diminish "procedural justice"—the perception that legal authorities act fairly[30]—and increase "legal estrangement," the sense among heavily policed communities that the law is not protective but punitive.[31] The opacity of these systems erodes individuals' ability to meaningfully challenge or confront algorithmic tools they cannot examine, understand, or test. In these ways, modern surveillance undermines foundational constitutional commitments to autonomy, equality, and democratic participation even before technological error enters the picture.

THE HARMS OF SURVEILLANCE ARE THEREFORE NOT ABSTRACT: THEY ARE IMMEDIATE, CONCRETE, AND OFTEN IRREVERSIBLE.

In ordinary life, data collected for mundane or administrative purposes can be repurposed in ways that endanger everyone. Political conditions can transform data collected, stored, and used by the state for benign purposes into a weapon. The government's collection and possession of our personal data give it the ability to monitor every individual and to know things that no government should. Even discrete pieces of data about an individual's health, finances, religious affiliation, or political activity can reveal intimate and detailed information to the state about who we are and what our lives look like. When aggregated, such data enables the government to map our movements, infer our habits, and reconstruct the texture of our private lives.[32] When surveillance technologies are used indiscriminately and without oversight, they turn ordinary exercises of personal freedom into potential grounds for state intrusion.

HARMS IN THE CRIMINAL CONTEXT

We need not speculate about the risks of state collection and use of incomplete, out-of-context, or inaccurate data. Misidentifications in facial recognition systems have led to wrongful arrests, police violence, and incarceration.[33] For example, Nijeer Parks was arrested in New Jersey after facial recognition misidentified him as a suspect in a shoplifting incident, despite his being 30 miles away at the time. He spent ten days in jail and faced decades in prison before charges were dropped.[34]

Cases like Mr. Parks's highlight how state collection and use of data can devastate lives, and how its harms extend well beyond the individual. As Professor Michael Pinard documents, the collateral consequences that flow from criminal system contact compound across families and communities and fall most heavily on communities of color, entrenching cycles of instability and diminished dignity.[35] Wrongful arrests fracture families, cost people jobs and relationships, and inflict long-lasting reputational and health harms.[36]

Unregulated data systems increase the risk that innocent people will be swept into criminal investigations, as aggregated digital traces can be reinterpreted or misused despite the absence of any suspicion of wrongdoing.[37] Sociology professor Sarah Brayne describes this as "dragnet surveillance"—routine, cumulative, and suspicionless monitoring made possible by automated data capture across entire populations.[38]

These unchecked systems provide officers automated "alerts" about individuals based on algorithmic matches or the appearance of certain data points, shifting surveillance from reactive querying to continuous, real-time monitoring.[39] By converting ordinary digital behaviors into potential investigative leads, these tools expand the reach of the criminal legal system far beyond traditional thresholds of suspicion.

BY CONVERTING ORDINARY DIGITAL BEHAVIORS INTO POTENTIAL INVESTIGATIVE LEADS, THESE TOOLS EXPAND THE REACH OF THE CRIMINAL LEGAL SYSTEM FAR BEYOND TRADITIONAL THRESHOLDS OF SUSPICION.

As described, facial recognition technology has resulted in numerous misidentifications, causing a host of carceral consequences. The flaws of facial recognition technology are not isolated. DNA databases are riddled with errors, duplicate entries, and misattributed samples that disproportionately affect people of color, whose DNA is overrepresented due to biased policing practices.[40] ShotSpotter, an algorithmic gunshot detection system, has generated false alerts that police treat as evidence of crime. In Chicago, Michael Williams spent nearly a year in jail after being wrongfully charged with murder based on a ShotSpotter alert later shown to be erroneous.[41]

Location data from phone apps (for example, popular games like Candy Crush that are integrated with ad-tracking software development kits) are routinely sold through brokers like Gravy Analytics, which have marketed those datasets to U.S. law enforcement agencies.[42] Wearable fitness-tracker data has been used in criminal cases to build timelines and test alibis,[43] and similar data could easily be subpoenaed for immigration and family law investigations.[44]

DISPROPORTIONATE IMPACT

The state's use of our data can transform structural bias into seemingly objective data. In Allegheny County, Pennsylvania, the Department of Human Services' *Family Screening Tool* uses hundreds of public datasets to predict a family's risk of child neglect or abuse.[45] Yet because those datasets reflect entrenched racial and socioeconomic disparities, such as correlations between poverty, policing, and child welfare reporting, the algorithm disproportionately flags low-income, Black, or other marginalized families for investigation.[46] What appears as neutral, data-driven decision-making reproduces existing inequalities under the guise of technical precision.

Scholars have documented how predictive tools reinforce entrenched racial disparities in policing. Predictive tools are typically trained on police-generated enforcement data such as stops, arrests, and incident reports, which already reflect decades of racially disparate and sometimes unlawful policing practices.[47] Predictive algorithms learn from these patterns and then direct officers back to the same neighborhoods that were historically policed.[48] Empirical studies demonstrate this feedback dynamic. Predictive systems often "forecast" future policing rather than future crime because the algorithm's outputs simply mirror prior police deployment patterns.[49] One study found that even very small differences in initial enforcement levels can cause the algorithm to allocate nearly all future patrol resources to a single neighborhood, even when the true crime rate is identical across areas.[50] This pattern creates a self-reinforcing loop that reproduces past inequities and concentrates future enforcement on the same communities.

PREDICTIVE SYSTEMS OFTEN "FORECAST" FUTURE POLICING RATHER THAN FUTURE CRIME BECAUSE THE ALGORITHM'S OUTPUTS SIMPLY MIRROR PRIOR POLICE DEPLOYMENT PATTERNS.

Structural inequalities are not erased by data-driven tools; they are often encoded and amplified by them. Data sets feeding surveillance systems are not neutral reflections of social reality but products of longstanding disparities in policing and public administration. As scholars have noted, these systems inherit the racial and socioeconomic biases embedded in their training data, producing outputs that replicate and legitimize those inequalities under the guise of technical objectivity.[51]

Modern surveillance technologies widen these disparities by lowering the threshold for inclusion in law enforcement databases. Tools such as automatic license plate readers, video analytics, and commercially purchased dossiers sweep in individuals with no prior police contact, dramatically expanding the population subject to monitoring and suspicion.[52] Once included in these systems, individuals may be subject to associational inferences, query-based profiling, and network analyses that treat incidental, outdated, or context-free data points as indicators of risk. Repeated database queries, moreover, can become self-perpetuating markers of suspicion, as prior investigative attention is later cited to justify further scrutiny.[53]

THREATS TO FUNDAMENTAL RIGHTS AND VALUES AND THE NEED TO ACT

Many have acquiesced to the government having so much information about us. This report and the DJA serve as a reminder that we should not accept this as normal. Individuals retain a right to be let alone, a right to be forgotten, and a right to anonymity. The DJA seeks to vindicate those rights by erecting statutory safeguards that limit what data the state can collect, how long it can retain it, and how it may use it.

The absence of clear, enforceable rules around data collection and use creates profound uncertainty. Individuals cannot exercise meaningful autonomy or free expression when they do not know:

- What information is being collected;
- How data collection algorithms work;
- When and under what circumstances collection occurs;
- How data are stored, analyzed, or shared;
- For what purposes data are ultimately used;
- Whether data collected by private actors (such as wearable devices or health-tracking apps) may later be sold or transferred to the state;
- Who is collecting our data;
- If or when data are deleted; and
- How emerging technologies might manipulate or repurpose data in ways we cannot yet predict.

Artificial intelligence (AI)[54] compounds these concerns. Designers, manufacturers, and government AI users often lack insight into the decision-making processes of their own systems, creating what many call the "black box problem."[55] This opacity fosters a climate of self-censorship and restraint in which people avoid searching, reading, or associating in ways they otherwise would, out of concern that their data could later be used against them. The result is a slow erosion of democratic freedoms, where the fear of unseen watchers shapes behavior as powerfully as formal legal prohibitions.

Surveillance harms arise not only from isolated data points but from the ways state agencies aggregate and fuse disparate datasets into unified analytic environments. This fusion of public and privately collected records can be described as a form of "data laundering" because commercial data is repurposed for state investigative use. It helps explain the scale and analytic power of modern policing platforms. Commercial platforms like Palantir integrate information from previously siloed systems, such as field interview cards, records, automated license plate reader scans, crime reports, county jail logs, department of motor vehicles data, and even privately collected records.[56] Since Palantir combines government records with commercially sourced information, its interface allows officers to run a single query across sources that were never intended to be linked, allowing officers access to "hundreds of millions of disparate data points" within a single search.[57] This type of integration enables officers to generate profiles, associations, and investigative leads at remarkable speed by linking data across sources that were never designed to be used together.[58] Without limits on aggregation and reuse, this fusion of institutional and commercial data transforms ordinary life into a persistent set of interpretable digital traces, allowing police to reconstruct movements, relationships, and behaviors long after the original collection, and often without a person's knowledge or ability to consent.[59]

Taken together, these examples illustrate that the problem is not confined to one flawed tool or dataset, but to a surveillance ecosystem that enables state actors to collect, retain, and repurpose vast amounts of personal information with little oversight. State actors already enjoy expansive access to personal data. Piecemeal, technology-specific regulations or narrow evidentiary rules are important but will not suffice to limit the state's use and collection of personal data. Meaningful reform must limit the surveillance machinery at its source by focusing on the collection and retention of data. Only by limiting what private vendors may collect for government use *and* restricting how state agencies may access, retain, and repurpose that data once it enters government systems can the law effectively prevent the harms described.

LEGISLATIVE AIMS

Together, this report and the DJA articulate core principles grounded in two basic premises: personal data belongs to the individual, and the state's use of such data must be narrow, lawful, transparent, and accountable. These core principles establish: (1) rights and values protecting individuals and their data; (2) safeguards requiring necessity, proportionality, and independent oversight of state data collection and use; (3) limitations on retention and secondary data use; and (4) enforceable procedural rights and remedies. By embedding these principles in law, the DJA reins in the state's unchecked dominion over personal data, restores balance between government power and individual autonomy, and safeguards democratic values in the digital age.

INDIVIDUAL RIGHTS AND VALUES

THE RIGHT TO PRIVACY IN THE DIGITAL ERA

The constitutional right to privacy, rooted in the First, Fourth, and Fourteenth Amendments, must be reconceptualized for the digital era. Nearly a century ago, United States Supreme Court Justice Louis Brandeis observed that as new technologies create new ways to invade privacy beyond physical trespass, the Constitution's protections must evolve accordingly and recognized the government's duty to respect our "right to be let alone."[60] To protect this right, he presciently warned, "every unjustifiable intrusion by the government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment."[61]

The Supreme Court has begun to vindicate Justice Brandeis's insight and the need for a shift in how we understand privacy.[62] As the Court has explained, "a person does not surrender all Fourth Amendment protections by venturing into the public sphere."[63] Even so, persistent digital tracking provides a "detailed, encyclopedic, and effortlessly compiled" record of a person's life, and as the Court now acknowledges, long term surveillance creates a privacy harm.[64]

The problems extend beyond the bounds of the Fourth Amendment. Persistent monitoring and data collection also undermine rights guaranteed by the First and Fourteenth Amendments: freedom of association, expression, and equal protection. To address these threats, statutory protections must embrace a privacy model grounded in autonomy, dignity, and democratic participation. The DJA recognizes that a robust construction of privacy is a foundational element of democratic personhood.

COMPONENTS OF THE MODERN RIGHT TO PRIVACY

The modern right to privacy comprises several interrelated components that safeguard autonomy, dignity, and democratic principles. These include protection from persistent surveillance, the right to be let alone, the right to be forgotten, and the right to anonymity. Each of these components reflects distinct but complementary parts of the DJA's protection of privacy in the digital age.

Protection from Persistent Surveillance

The DJA recognizes that surveillance should be targeted, limited in duration, and legally justified, not constant and indiscriminate. All too often, modern surveillance begins long before any formal law enforcement inquiry. Ordinary digital traces, license plate readers, facial recognition, and other monitoring systems, create a constant stream of data as individuals move through the world.[65] These seemingly innocuous data points accumulate into detailed records that enable persistent, passive, and retrospective surveillance without individualized suspicion, particularly affecting communities that have been historically marginalized and overpoliced.

The Right to Be Let Alone

The DJA codifies the right to be let alone by prohibiting constant, suspicionless monitoring while mandating that all government data collection be justified as necessary and proportionate. When the government constantly monitors each of our locations, online behavior, and associations, it chills freedom of expression, movement, and association, diminishing the quality of democracy. This principle also recognizes that the government must affirmatively justify monitoring as narrowly tailored, necessary, and lawful.

ORDINARY DIGITAL TRACES, LICENSE PLATE READERS, FACIAL RECOGNITION, AND OTHER MONITORING SYSTEMS, CREATE A CONSTANT STREAM OF DATA AS INDIVIDUALS MOVE THROUGH THE WORLD.

The Right to Be Forgotten

The DJA establishes a right to be forgotten, mandating the automatic deletion of data once its lawful use has ended, such as after acquittal, the dismissal of charges, or the conclusion of an investigation.[66] It also requires the permanent destruction of unlawfully collected data, including any derivative data, and prohibits the repurposing of data. For example, data lawfully collected for one investigation cannot be reused for any other purpose under the DJA.[67] Privacy requires meaningful control over one's digital footprint; the DJA ensures privacy is not a temporary condition but a continuing right that persists even after data's lawful use has ended.

The Right to Meaningful Notice and Informed Consent

Procedural due process requires individuals to be given a fair opportunity to know of, question, and contest government action.

The DJA asserts that individuals do not forfeit due process rights simply by using digital services or participating in modern life, rejecting the third-party doctrine.[68] Too often, surveillance relies on purported consent buried in incomprehensible terms of service incompatible with due process, fairness, and the realities of modern life.

To ensure that individuals maintain meaningful control over their personal data, the DJA establishes clear standards for notice and consent that reflect ethical, constitutional, and technological realities. Meaningful notice requires that individuals be informed contemporaneously, at or near the time of data collection, not weeks or months later. Notice must be comprehensible, written in clear, plain language, and free from legal or technical jargon. It must also be specific, clearly explaining what data is collected, when the data is being collected, who is collecting it, the purpose of the collection, and how long the data will be retained.

Valid consent must be affirmative, informed, revocable, and voluntary. Silence or failure to opt out cannot be construed as consent. It must be informed, ensuring individuals fully understand what they are agreeing to without hidden terms. Consent must also be revocable, allowing individuals to withdraw it at any time, and voluntary, meaning it cannot be obtained through coercion or as a prerequisite for accessing services or exercising legal rights. Therefore, when access to near-essential and essential services, such as transportation, housing, or public benefits, is conditioned on individuals surrendering personal data, the "choice" to consent becomes coercive and moot.[69] For example, the "spit and acquit" practice used by the Orange County California District Attorney's Office where individuals charged with misdemeanors are offered dismissal of charges or a plea offer in exchange for giving the government their DNA is coercive and should not be considered consent.[70]

Importantly, even when individuals provide consent, constitutional doctrines limit their ability to override constitutional protections. The unconstitutional conditions doctrine recognizes that the government cannot condition access to benefits on the surrender of an existing right without limit.[71] In other words, consent cannot serve as a loophole to bypass constitutional safeguards.[72] This principle shows why seemingly voluntary agreements, such as mandatory data sharing to access public benefits or essential services, cannot be relied upon to justify rights violations.[73]

These principles reject opt-out usage of many current data systems, which presume consent. These principles also reject constructive consent frameworks where the government treats third-party data as exempt from privacy protections.

The DJA acknowledges that surveillance is not evenly distributed. Modern surveillance practices add to structural biases in digital systems and databases, reinforcing cycles of over-monitoring communities and incarceration, making equal protection violations a central concern in surveillance policy.

Equal protection principles require that surveillance practices not be deployed in ways that disproportionately burden specific groups. At the same time, constitutional standards also demand procedural safeguards to protect individuals when their data is collected, used, or reused. Yet, current surveillance systems fail on both fronts. To ensure equity and that constitutional standards are met, individuals must be afforded procedural rights whenever their data is collected, used, or reused.

The DJA acknowledges that procedural safeguards and the principles of equal protection must be codified, enforceable, and accessible.

These safeguards require:

- Advanced notice of data collection;
- The ability to challenge the legitimacy, relevance, and accuracy of the data being used;
- The ability to contest the inclusion of data in law enforcement tools, such as predictive law enforcement tools or gang databases;
- The ability to appeal data-related decisions;
- The ability to challenge the reliability of technologies;
- Government actors to keep thorough records detailing the use and deployment of surveillance tools, the types of data collected, and the duration for which the data is retained; and
- Regular audits, independent review boards, and public reporting to accompany the use of all surveillance systems.

The Right to Contest Algorithmic Decision-Making

Algorithms are frequently flawed and can produce harmful consequences.[74] For instance, facial recognition technology tends to be less accurate for people of color.[75] Similarly, automated pre-trial risk assessment tools—which analyze factors such as age, prior convictions, employment status, zip code, and neighborhood crime—to generate risk scores by comparing an individual's data to past cases, often produce inaccurate and biased results.[76] These tools disproportionately assign higher risk scores to people of color accused of crimes and low-income individuals, perpetuating discriminatory outcomes.[77]

Democracy requires that individuals are able to contest decisions that affect their life, liberty, or livelihood. The Due Process Clauses of the Constitution require these decisions to be transparent, reviewable, and fair. Use of data-driven algorithms for decision-making requires procedural safeguards that allow meaningful review. Accordingly, individuals must have the right to challenge algorithms' training data, especially when it reflects historical discrimination or flawed law enforcement practices, and to scrutinize algorithms' underlying logic, assess error rates and bias metrics, and contest results.

The DJA asserts that no individual should be subject to any legal consequence based on automated decision-making. Algorithmic outputs should never be treated as dispositive evidence.

The Right to Personal Data Ownership

In the modern era, personal data is one of the most revealing aspects of individual identity. Personal data no longer merely reflects discrete features of who we are; it functions as a medium through which our full identities can be constructed. Despite the deeply intimate nature of this information, existing legal frameworks often treat personal data as a resource to be extracted, shared, or sold rather than as an extension of the self that demands protection and respect.[78]

Personal data is not only deeply intimate but also intrinsically valuable, akin to other intangible forms of property. Just as copyright protects creative expression, and the right of publicity protects someone's name, voice, and likeness, personal data should similarly be understood as an asset subject to legal protections. Tennessee's Ensuring Likeness, Voice, and Image Security (ELVIS) Act serves as an illustration of this concept. The Act recognizes a property right in a person's name, photograph, voice, or likeness, even including AI-generated likenesses.[79] This reflects a broader legal recognition that identity itself can be property. Extending this logic makes clear that personal data should not be treated as a public good to be extracted, but an extension of identity that demands legal guardrails and enforceable ownership rights.

PERSONAL DATA IS NOT ONLY DEEPLY INTIMATE BUT ALSO INTRINSICALLY VALUABLE, AKIN TO OTHER INTANGIBLE FORMS OF PROPERTY.

The harms of failing to recognize data as property, tangible or not, and instead treating it as a public good already manifest in law enforcement and government practices. The government can acquire personal data from private sector databases. This practice of unchecked government acquisition of personal data is magnified by the fact that such data can be used to justify deportation, surveillance, arrest, and incarceration. These are not hypothetical concerns.[80] For example, the Department of Defense has purchased location data from Muslim dating and Quran apps to surveil Muslim communities.[81]

A growing body of scholarship recognizes data as an intangible asset that can and should be governed through property-like concepts. Professors James Grimmelmann and Christina Mulligan argue that data already qualifies as a legally cognizable asset, because individuals can exercise control over it, transfer it, and suffer legally recognizable harms when that control is undermined.[82] In this sense, data functions like other forms of intangible property: it can be wrongfully taken, accessed, altered, or destroyed without authorization, giving rise to legal injury. Even critics of infusing personal data with the features essential to property rights acknowledge that the state has long created property interests in informational assets to address market failures or to incentivize production, suggesting that limited property interests in personal data can serve important governance functions while avoiding the risks associated with treating data as a fully alienable, marketable commodity.[83]

There are two primary ways the DJA conceptualizes personal data as property. The first is the traditional property model, which envisions data as a tangible asset over which an individual exercises exclusive control, akin to ownership of physical property. The second is the intellectual property model, which views data as an intangible asset with economic, creative, and informational value, incorporating doctrines of copyright, trade secrecy, and the right of publicity. Integrating intellectual property and traditional property conceptions of data ensures that ownership of personal data remains both meaningful and enforceable in the digital age by grounding individual control over data in established legal doctrines that recognize exclusion, limit unauthorized use, and provide remedies when those limits are violated.

The DJA makes clear that individuals own their personal data. Personal data is an individual's property and not freely available for government collection or use. While there are ongoing debates about whether data should be conceptualized as property,[84] these discussions persist because personal data defies traditional notions of ownership. American law has typically addressed data through contract and tort principles rather than property law.[85] Nevertheless, this framework emphasizes ownership to ensure robust, enforceable protections against government overreach.

Under longstanding principles of American law, the government cannot seize property without lawful justification and due process.[86] By extension, the state should not be permitted to seize or access personal data without explicit legal authority and procedural safeguards. The taking, aggregation, transfer, and collection of personal data should be subject to legal scrutiny. Accordingly, established common law doctrines such as trespass, which protects against unauthorized interference with one's possessions, and bailment, which imposes duties of care and limits on the use of property

entrusted to another, should likewise extend to personal data. Sharing personal data, whether by using a social media platform, or other everyday actions, should not negate an individual's ability to access, retain, or repurpose that data. Personal information does not become public property simply because it has been shared.

Personal data ownership carries with it a bundle of rights that includes:

- The right to know who has accessed one's data;
- The right to control how it is used, stored, and disseminated;
- The right to exclude others from accessing, transferring, or using the data without consent;
- The right to limit reuse, for example when data is repurposed in ways that differ from the original justification for collection; and
- The right to revoke access by demanding deletion or return of personal data once the lawful basis for its retention has ended.

When the government transfers personal data to third parties, retains personal data obtained from third parties, incorporates personal data into learning models, or stores personal data in databases without clear legal authority, its actions constitute a taking and a seizure of property. Ownership of personal data imbues it with the due process protections afforded to property.

LIMITATIONS ON STATE USE OF DATA

STATE ACTORS MUST NOT INDEFINITELY RETAIN OR MISUSE PERSONAL DATA

State interests must be balanced against individuals' right to control their personal information. State agencies wield uniquely coercive powers, and their ability to collect, analyze, and retain personal data poses distinct risks to civil liberties that demand explicit statutory constraints. The accumulation of personal information, even when lawfully collected, creates a surveillance infrastructure that transforms temporary investigative tools and seemingly innocuous systems into permanent dossiers on individuals and entire communities.

Without strict limitations, state agencies routinely repurpose data collected for one purpose to serve entirely different, intrusive ends.[87] This form of data laundering also allows police to circumvent constitutional protections and democratic norms by using privately collected data gathered for non-law enforcement purposes in criminal investigations.[88] For example, in New Orleans, police secretly deployed a private network of facial recognition cameras operated by a nonprofit organization to conduct real-time surveillance and make arrests.[89] This practice violated the city's surveillance ordinance requiring judicial oversight and disclosure. By partnering with the private entity Project NOLA, police evaded accountability mechanisms and created a surveillance regime that operated outside democratic control for two years before public disclosure forced its suspension.[90]

Retention and Use Limitations

The state may only collect and use data for the specific, limited purpose for which it was lawfully authorized, and cannot repurpose or reuse it without explicit legal authority. Personal data must not become a permanent asset of the state. The retention of information long after its legitimate use has expired risks converting temporary investigative tools into permanent dossiers on individuals and communities.

This principle prevents data collected for one purpose from quietly migrating into unrelated law enforcement priorities, training datasets, or intelligence operations.

Destruction of Personal Data

Unlawfully obtained data must be immediately and permanently destroyed, including all copies, derivatives, and any outputs from algorithmic systems trained on that data. Lawfully obtained data must be sealed once its authorized legal purpose has concluded. Sealing triggers automatically upon (1) completion of the investigation or proceeding; (2) acquittal, dismissal, or declination of charges; or (3) expiration of the time period authorized for retention, whichever occurs first. Sealing restricts government use and disclosure, but it does not bar the individual whose data is at issue from accessing, obtaining, or reviewing that data.

Elimination of Unauthorized Databases and Learning Models

Unauthorized databases and learning models must be eliminated. State actors cannot maintain databases or train machine learning models using personal data collected without compliance with this legislation. Existing databases compiled in violation of these principles must be audited and, where unlawful, dismantled. Algorithmic systems trained on improperly collected data must be retrained or decommissioned. The state cannot launder unlawfully obtained information by incorporating it into predictive models or intelligence systems.

Validation of Data Collection and Use Technology

Technologies used for surveillance or for other data collection and use purposes must be validated before use. Courts have long required scientific evidence to meet reliability standards before admission.[91] Yet surveillance technologies often evade judicial scrutiny because their use is not disclosed or necessary to be admitted as evidence.[92] Before any surveillance technology may be deployed or used by state actors, it must undergo rigorous, independent validation to demonstrate accuracy, reliability, and freedom from systemic bias.[93] Validation must be conducted by neutral third parties, rather than vendors or law enforcement agencies, and results made publicly available. Reliability standards must include disclosure of all appropriate error rates, false positive/negative rates, demographic disparities, and limitations of the technology.

STATE ACTORS MUST DISCLOSE ALL COLLECTED DATA TO ACCUSED PERSONS AND COURTS.

Transparency is essential to adversarial testing and due process. State actors must disclose to accused persons and courts all personal data collected, accessed, or analyzed in connection with a case—including data held by private vendors, contractors, fusion centers, or partner agencies at any level of government. This duty extends to:

- The fact of surveillance and data collection;
- The categories and sources of data obtained;
- The technologies, algorithms, and analytical methods employed;
- Any third parties with access to the data;
- The chain of custody and any modifications to the data;
- Error rates, reliability testing, and validation studies for any technology used; and
- All exculpatory information revealed through data analysis.

As scholars have pointed out, pretrial notice and disclosure enables accused persons to challenge the reliability of technological evidence and ensure that fact-finders understand the limitations and potential biases of algorithmic systems.[94] Failure to disclose should be grounds for exclusion of evidence and sanctions. The prosecution cannot withhold information about surveillance practices, vendor contracts, or algorithmic decision-making on grounds of proprietary business information, law enforcement sensitivity, or administrative burden. Scholars have stressed the degree to which private control of big databanks and search capabilities has limited state actors from proper transparency in the legal system.[95] Proprietary protections such as copyright and trade secrets shield commercial databases and algorithms from independent scrutiny, as private companies maintain secrecy to preserve competitive advantages and prevent reverse engineering.[96] These intellectual property safeguards create systemic opacity that extends even to law enforcement contracts, where nondisclosure provisions prevent public examination of the technologies and data compilations that shape criminal investigations.[97] This disclosure requirement aims to prevent law enforcement from relying on private technological systems whose design, data inputs, or error rates cannot be independently tested, ensuring that only evidence subject to full transparency and independent review may be used in court.

PROPRIETARY PROTECTIONS SUCH AS COPYRIGHT AND TRADE SECRETS SHIELD COMMERCIAL DATABASES AND ALGORITHMS FROM INDEPENDENT SCRUTINY, AS PRIVATE COMPANIES MAINTAIN SECRECY TO PRESERVE COMPETITIVE ADVANTAGES AND PREVENT REVERSE ENGINEERING.

SAFEGUARDS

The status quo of modern data collection and use can render constitutional and statutory rights illusory. To give effect to the individual rights and values outlined above, the DJA establishes safeguards to govern data collection, use, and disposal by state actors.

NECESSITY, SPECIFICITY, AND PROPORTIONALITY

All government data practices must meet standards of necessity, specificity, and proportionality. The burden is on the government to show that data collection is narrowly tailored and necessary for a legitimate investigative purpose. Collection must be time-bound and cannot extend beyond the stated justification.

LOGGING AND ACCESSIBILITY

Every instance of personal data access by a government actor must be recorded in an auditable system accessible to courts, individuals, and the public. Records must document who accessed the data, when it was accessed, for what purpose, and how the data was used.

OVERSIGHT

Without independent oversight, government actors can deploy intrusive tools without accountability or public scrutiny. Independent oversight helps ensure that data collection programs stay within legal bounds, are regularly assessed, and respond to community concerns. Independent oversight bodies must be empowered with genuine authority, not reduced to entities that rubber-stamp government decisions.

Independent oversight bodies must include representation from the communities most impacted by surveillance, such as low-income, Black and Latine, and other communities policed at disproportionately high rates. This report acknowledges the challenges of achieving meaningful community representation in practice.[98] Community member perspectives must carry weight and community members must have real decision-making authority. Accordingly, oversight agencies should not be controlled by or dependent on the entities they seek to monitor. Their funding, staffing, and authority must be insulated from law enforcement and political influence. No new surveillance tool may be acquired or used without prior community input, transparency, and approval.

ALGORITHMIC TRANSPARENCY

Meaningful oversight also requires algorithmic transparency. Community members and oversight bodies must be able to understand, evaluate, and challenge the logic of algorithms used to collect, aggregate, or analyze personal data. Accordingly, no algorithmic system should be deployed in a surveillance or enforcement context unless its design, inputs, and decision-making processes are disclosed and subject to review.

PROCEDURAL RIGHTS AND REMEDIES

Individuals have the right to meaningful remedies when their data rights are violated. Remedies are essential to ensuring fairness and compliance. Without enforceable remedies, the rights and procedural safeguards outlined above risk becoming aspirational rather than actionable.

The DJA acknowledges that individuals must have access to timely, thorough notice and the ability to contest collection, retention, and use. Notice, access, and the right to challenge are fundamental data rights that cannot be waived through plea bargains, coercion, or form terms of service. Where data rights are violated, meaningful remedies include suppression, deletion, and civil damages.

CIVIL CAUSE OF ACTION

To guarantee enforceability, the DJA creates a private right of action for individuals whose personal data has been unlawfully collected, retained, shared, or used by government actors. Each individual who falls into this category has direct standing to sue. The cause of action applies against private actors who contract with, act on behalf of, or materially assist government entities such as data brokers and vendors that contract with or assist the government in surveillance and data analysis. Individuals whose personal data has been unlawfully collected, retained, or shared shall have access to monetary damages and/or injunctive relief.

COLLECTIVE REDRESS

To address systemic data abuses, collective remedies must also be permitted. Because surveillance programs, automated decision-making systems, and data sharing practices often apply uniformly across broad populations, individuals are likely to face the same harms stemming from the same underlying policies or technologies. Thus, the DJA explicitly allows for class action lawsuits to address situations in which data collection policies affect large groups of individuals. Class actions provide an efficient mechanism to adjudicate these claims simultaneously.

EVIDENTIARY LIMITS, GOVERNMENT ACCOUNTABILITY, AND DATA DESTRUCTION

To preserve due process rights, evidence derived from unlawfully collected, undisclosed, or unreliable data must be excluded from criminal proceedings. Unreliable data includes, but is not limited to, data that is inaccurate, biased, unverified, or produced by technologies lacking scientific validation.

The government must not benefit from violating individual rights or evading legal scrutiny through partnerships with third-party vendors. Accordingly, prosecutors must disclose all personal data collected or accessed in the course of an investigation. This duty applies to data in state possession or

control or in the possession or control of third-party entities that support or assist law enforcement, family regulation, or corrections agencies. Under the DJA, prosecutorial data disclosure obligations apply to data of parolees, pre-trial detainees, and individuals under court-ordered supervision.

Courts must exclude evidence derived from unlawfully collected, undisclosed, or unreliable data. Moreover, for any criminal investigation or case that concludes without a conviction, for example by acquittal, dismissal of charges, or the end of an investigation, all personal data gathered in connection with a criminal investigation must be automatically and permanently destroyed, not merely archived. No residual files or derivative databases may be retained. In addition, individuals must have access to clear, timely, and accessible processes to file complaints concerning data misuse, inaccuracies, or unauthorized retention, including the right to request correction or deletion and to appeal adverse decisions.

DEBUNKING MYTHS

MYTH 1: SURVEILLANCE TOOLS HELP EXONERATE INNOCENT PEOPLE

While some exculpatory data can play a role in clearing individuals of wrongdoing, surveillance tools also collect vast amounts of data that expose innocent people to heightened risk and scrutiny.[99] The current scale of surveillance that reveals the occasional exculpatory evidence is not justified. The DJA ensures that data essential to criminal investigations remain available, while preventing overcollection and indefinite retention that threatens privacy, equality, and due process.

MYTH 2: SURVEILLANCE IS INEVITABLE, SO REGULATION IS POINTLESS

Surveillance is not inevitable; it is the result of policymaking. Since data collection has expanded so rapidly, comprehensive safeguards are more necessary than ever. What begins as routine monitoring, tracking movement through devices, social media activity, or physiological data from apps, can be repurposed in ways that invade privacy, chill free expression, and target marginalized communities.[100] The absence of regulation has created and deepened power imbalances, enabling state actors to collect, retain, and repurpose personal data without democratic accountability.[101]

Regulation provides a meaningful way to direct and limit surveillance practices, countering the claim that they are beyond democratic control. Left unchecked, these practices embed structural inequalities as ordinary activities become sources of constant surveillance and individuals are chilled from fully participating in civic, social, or political life.[102] The DJA provides the statutory limits and protections that state collection and use of personal data requires.

MYTH 3: IF YOU HAVE NOTHING TO HIDE, YOU HAVE NOTHING TO FEAR

This argument misunderstands how surveillance works and who it harms. Most modern surveillance systems operate upstream, collecting, storing, and analyzing data about everyone regardless of conduct or the existence of suspicion. Even data initially collected for routine or seemingly benign purposes, like social media posts, movement through public spaces, or physiological data from apps, can be repurposed to track, target, or penalize individuals long after collection, producing chilling effects, and exacerbating structural inequalities.[103] Moreover, civil liberties are not conditioned on a person's conduct, they exist to protect everyone against state overreach. The DJA safeguards the right to be let alone and to be free from suspicionless monitoring, cornerstones of a democratic society.

MYTH 4: MORE DATA LEADS TO MORE NEUTRAL AND OBJECTIVE POLICING

Data is not neutral, it amplifies existing racial, economic, and geographic disparities.[104] Predictive tools and databases often reproduce their own assumptions, creating self-reinforcing cycles of policing in already over-policed communities. When the inputs themselves reflect structural biases, the outputs do not reflect fairness or legitimacy.[105] The DJA ensures that data systems do not automate discrimination under the guise of neutrality.

MYTH 5: OVERSIGHT OF DATA SURVEILLANCE WILL HINDER PUBLIC SAFETY

Effective oversight of data surveillance will actually strengthen public safety by improving accuracy, reducing errors, and maintaining public trust. Unchecked systems produce false positives and wrongful arrests, and thus misdirect enforcement efforts in ways that waste resources and undermine the legitimacy of state actors. The DJA's safeguards, including transparency, necessity, proportionality, and independent oversight, ensure that surveillance tools are used responsibly, lawfully, and in ways that strengthen community safety.

CONCLUSION

The current data collection landscape is dangerous because it threatens individual rights, democratic values, and undermines racial justice. Digital technologies have rapidly outpaced legal protections, enabling pervasive government surveillance without transparency or accountability. These practices extend a long and painful legacy of discriminatory policing and state control, further embedding structural inequalities into everyday life.

The DJA confronts these challenges directly. It re-centers both individual rights and democratic principles as the foundation of digital governance, addressing mission creep, demanding accountability, and drawing clear boundaries the government must not cross. The status quo must change. There is both a legal and moral imperative to act. This legislation is necessary to preserve privacy, due process, equity, and justice in the digital age. The path forward is clear: policy makers must act with urgency to enact the DJA's protections and ensure that the state's power to amass and use our personal data no longer remains unchecked.

ACKNOWLEDGMENTS

The model legislation reproduced in the Appendix and discussed in this report predates this project. The idea for the legislation originated more than three years ago as an exercise in liberatory imagination and collaborative drafting between Elizabeth Daniel Vasquez and Maneka Sinha, who jointly developed and authored the initial bill text. That text was incorporated into this report as the Data Justice Act.

We express our sincere gratitude to those who contributed to the development of this report:

- The members of the Fall 2025 Forensic Defense Clinic: Yuri Ceriale, Kaitlin Ponder, Rhea Sahai, Garrett Salzman, Sabat Siddiqi, and Michela Weihl;
- Virginia Ryan (NYU Law '27);
- Professor Cristopher Moore;
- Professor W. David Ball;
- Professor Kate Weisburd;
- Professor Chris Morten;
- Professor David Reiss; and
- Nathan Freed Wessler.

We are deeply grateful for the expertise each contributor offered. Their commitment to advancing thoughtful, rights-protective approaches to data governance made this project possible.

APPENDIX: THE DATA JUSTICE ACT

AN ACT TO RESTRICT THE COLLECTION AND RETENTION OF PERSONAL DATA BY STATE ACTORS

WHEREAS, the [Council] finds that the unchecked collection and use of personal data by state entities threatens fundamental rights to privacy, autonomy, and equality.

WHEREAS, the [Council] finds that, under the guise of promoting public safety, state actors routinely and continuously collect massive amounts of individualized data about residents of and visitors to the [City/County/State].

WHEREAS, the [Council] finds that state actors indiscriminately collect this data about all residents and visitors, including parolees, individuals awaiting trial, and other persons under state supervision, not only those suspected of criminal involvement.

WHEREAS, the [Council] finds that the data collected by state actors is vast, and includes myriad intimate and personal details about individuals' appearance, genetic information, health conditions, locations, movements, activities, finances, employment, relationships and social networks, health, and more.

WHEREAS, the [Council] finds that state actors routinely and continuously collect such individualized data surreptitiously, in secret, and without individual consent.

WHEREAS, the [Council] finds that state actors collect individualized data using a myriad of sophisticated technologies.

WHEREAS, the [Council] finds that state actors use such individualized data to surveil and monitor [City/County/State] residents and to make predictions about individuals' future activities and conduct.

WHEREAS, the [Council] finds that state actors have created a vast and immensely detailed surveillance network through the continual collection, storage, and aggregation of individual data.

WHEREAS, the [Council] finds that state actors retain individual data long after the original justifications for collection cease to exist, often endlessly, and without limitation or any policy or regulation requiring purging such data.

WHEREAS, the [Council] finds that individuals residing in and traveling through the [City/County/State] have an interest in knowing what individualized data about them is collected.

WHEREAS, the [Council] finds that surveillance and monitoring impose harm on all those subjected to it, including by diminishing individuals' ability to live anonymously and free of government scrutiny.

WHEREAS, the [Council] finds that harm to individuals flows from the collection of individualized data itself, not only from the use of specific technologies to acquire or analyze such data.

WHEREAS, the [Council] finds that surveillance and monitoring have historically been disproportionately applied to Black, Latine, indigenous, and other minoritized and marginalized communities.

WHEREAS, the [Council] finds that in order to promote the safety and wellbeing of the citizenry, it is necessary to restrict the collection and retention of data by [City/County/State] agencies.

WHEREAS, the [Council] finds modern surveillance technologies undermine constitutional guarantees of due process and equal protection.

WHEREAS, the [Council] finds that individuals retain ownership and control over their personal data, which constitutes an extension of self and liberty interests protected under the Fourth and Fourteenth Amendments.

THEREFORE BE IT RESOLVED:

SECTION 1. SCOPE AND APPLICATION.

This Act proscribes the collection and use of personal data, as defined by Section 2. This Act applies to all personal data, regardless of the technology, device, or tool used to acquire it, or the entity or agent that acquires it.

This Act applies to all collection, use, analysis, or retention of personal data by or on behalf of any public authority, including through private contractors, vendors, or data brokers acting under color of law.

A. The provisions of this Act apply to all [City/County/State]:
    1. Law enforcement entities, to include police departments, investigative agencies, and prosecutors' offices;
    2. Corrections agencies;
    3. Court supervision agencies, including probation, parole, and pre-trial supervision offices;
    4. Child protective and child welfare agencies;
    5. And other state actors.

B. This Act prohibits the voluntary distribution, transfer, or sale of personal data by any agency described in Section 1, Subsection A to any third-party company, corporation, entity, or federal authority, including federal immigration agencies.

SECTION 2. DEFINITIONS.

For purposes of this Act:

A. "Collection and use" shall mean any action, whether taken digitally or by a human, that results in any form of access to personal data and/or that relies in any way on personal data for decision-making, analysis, or action. This includes, but is not limited to, direct operation of a surveillance tool, as well as receiving, accessing, analyzing, or otherwise relying on data, results, or outputs produced by the tool, whether obtained internally or from a third party.

B. "Critical categories of personal data" shall include:

1. Genetic information, which means information about (i) an individual's genetic profile, genetic analysis, or inherited traits, (ii) the genetic tests of an individual's family members, and (iii) the manifestation of a disease or disorder in an individual's family members;
2. Biometric information, which means information about an individual's observable or measurable intrinsic biological traits or characteristics, including but not limited to, fingerprints, handprints, retina and iris patterns, DNA sequence, voice, gait, and facial geometry;
3. Other health-related information, which means information related to an individual's past, present, or future physical or mental health status, including, but not limited to, medical history, diagnoses, treatments, medications, disability status, substance use history, reproductive health, or HIV status, plus any health-related categories developed in the future;
4. Location information, which means information concerning an individual's past, present, or future physical or digital location or movements, travel routes, objects of geolocation, or travel patterns, plus any location-related categories developed in the future;
5. Associational information, which means information about, including but not limited to, an individual's personal relationships, communications, affiliations, memberships, or social networks, including predictive data, plus any associational categories developed in the future;
6. Other speech or thought-related information, which means information about an individual's public or private speech, opinions, beliefs, thoughts, interests, or political views.

C. "Database" shall mean any repository of personal data, and "databasing" shall mean any action, whether taken digitally or by a human, that submits, searches, enrolls, or stores personal data to or in a database.

D. "Destruction" shall mean the permanent deletion of every instance and all copies, including backups and de-identified instances, of personal data by any entity, agency, or individual who has collected, stored, or used that personal data in any way.

E. "Due diligence" shall mean the good-faith (i.e., honest, non-pretextual), proactive, and reasonable (i.e., consistent with what a similarly situated entity exercising ordinary care would undertake) efforts taken by an entity or individual to identify, evaluate, and fulfill legal obligations under this Act. This includes, but is not limited to:
   1. Identifying all relevant data: Locating and accounting for all personal data within the entity's custody or control, including data held by contractors, vendors, and other government entities;
   2. Verifying legal authority: Confirming that all forms of collection, use, or distribution of personal data are authorized by law;
   3. Assessing risks of harm: Reviewing the potential for misuse, re-identification, or discriminatory impact of any collection or use of personal data, to be conducted by independent experts, oversight bodies, or other designated assessors as specified by regulation;
   4. Documenting efforts: Maintaining written records of the steps taken to comply with the notice, consent, data minimization, and destruction provisions of this Act;
   5. Other measures: Any other practices consistent with applicable law and established principles of transparency, fairness, and minimization of harm, including but not limited to steps to mitigate bias, prevent re-identification, and ensure accountability.

F. "Lawfully taken or seized personal data" shall mean personal data taken or seized in compliance with Section 3(A)(1) of this Act; "unlawfully taken or seized personal data" shall mean critical categories of personal data taken or seized in any other manner, including, but not limited to, data that is:
   1. Acquired through pretextual stops, coercive questioning, or informal interrogation;
   2. Purchased from commercial data brokers without individualized lawful authority;
   3. Accessed through third-party platforms or services without a warrant or statutory authority;
   4. Collected through passive and/or bulk surveillance;
   5. Shared between agencies or jurisdictions without legal authority for the transfer; or
   6. Retained beyond the legal time period permitted for lawful possession.

G. "Learning model" shall mean analysis, whether digital or human, developed from or trained with personal data.

H. "Personal data" shall mean any information or intelligence, regardless of how it is collected, generated, recorded, processed, retained, purchased, or otherwise obtained by a governmental department or entity, that is or was associated with, or is or was capable of being associated with, any specific individual or group of individuals. De-identification does not exclude personal data from this definition.

I. "Reuse" shall mean any action, whether taken digitally or by a human, that relies on personal data collected or used for one purpose for a different purpose.

J. “Sealing” shall mean the creation of a singular archived version of the personal data and transfer of that singular archived version to the confidential custody of the municipal archives, followed by the deletion of all remaining database instances and all copies, including backups, of the data contained therein by any other law enforcement or governmental entity; “sealed personal data,” even if it has been de-identified, cannot be used or maintained for any purpose by any governmental entity and can only be maintained by the municipal archive for the purposes outlined herein.

K. “Surveillance technology” means any hardware, software, or other system that collects, analyzes, generates, or stores personal data for the purpose of monitoring, predicting, or influencing individual or group behavior, including but not limited to facial recognition, DNA analysis, license plate readers, predictive policing systems, and algorithmic learning models.

L. “Unlawfully taken or seized personal data” shall mean personal data that has been unlawfully collected, purchased, accessed, shared, or retained without judicial authorization or other individualized lawful authority, including but not limited to:
   1. Data acquired through pretextual stops, coercive questioning, or informal interrogation;
   2. Data purchased from commercial data brokers without individualized lawful authority;
   3. Data accessed through third-party platforms or services without a warrant or statutory authority;
   4. Data collected through passive and/or bulk surveillance technologies, including closed learning models not ingesting agency data;
   5. Data shared between agencies or jurisdictions without legal authority for the transfer;
   6. Data retained beyond the legal time period permitted for lawful possession.

Individualized lawful authority means authorization based on specific judicial or statutory approval for a particular person or dataset, such as a warrant, court order, or statutory authorization.

Individualized lawful authority is required of both government and private actors, acknowledging distinct legal standards while recognizing the convergence of public and private surveillance infrastructures.

M. “Validation” means independent, pre-deployment testing by an entity with no financial or institutional interest in the technology’s adoption, demonstrating that the technology meets reliability, accuracy, and bias-mitigation standards established by law.

N. “Voluntary distribution, transfer, or sale” shall mean any action, whether taken digitally or by a human, that is not specifically required by law, which results in another entity having any form of access to personal data and/or relying in any way on personal data to achieve any result.

SECTION 3. DEFINING A PROPERTY INTEREST IN PERSONAL DATA.

A. Personal data ownership. Individuals are the owners of their personal data. Possession, access, or analysis by the state does not transfer or diminish ownership. These ownership rights explicitly include parolees, pre-trial detainees, and all individuals under any form of state supervision.
   1. Critical categories of personal data cannot be taken or seized from an individual without:
      i. Notice, as defined in Subsection C,
      ii. Due process, as defined in Subsection D, and
      iii. Lawful authority for the taking or seizure.
   2. Even when personal data is lawfully seized by any entity defined in Section 1(A), that personal data remains the property of the individual.

B. Personal data rights. In addition to personal property rights, individuals also have the right to privacy in their own personal data, the right to be anonymous, and the right to be forgotten.

C. Required notice.
   1. Notice.
      i. The entities described in Section 1 shall disclose their collection and use, databasing, reuse, use in a learning model, or distribution, transfer, or sale of critical categories of personal data to all individuals or groups currently or previously capable of being associated with such data.
      ii. The provisions of Section 3(C) apply to each entity that collects and uses, databases, reuses, uses in a learning model, or distributes, transfers, or sells critical categories of personal data, even if that entity received the personal data from another entity subject to the provisions of this Act.
   2. Notice requirements. Disclosure shall be made in writing and shall include:
      i. The identity of the entity conducting the collection and use activities and the date or date range(s) of collection and use of personal data;
      ii. A clear description of what personal data was collected and used, including designation of which critical categories of personal data are implicated;
      iii. A clear description of how the personal data was collected and used, including whether the collected and used personal data was databased, used in a learning model, reused in any way, or distributed, transferred, or sold;
      iv. The identities of any entities to which the personal data was distributed, transferred, or sold;
      v. A clear description of the legitimate governmental purpose pursued by the taking or seizure of the personal data;
      vi. The time period for which the entity intends to store the personal data;
      vii. Procedures by which persons can object to collection and use; and
      viii. Procedures by which personal data can be sealed and/or destroyed.

3. Timing. Disclosures required under this Section shall be made at the time when the initial collection and use occurs. Where an entity described in Section 1 intends to further collect and use, database, reuse, use in a learning model, or distribute, transfer, or sell that previously collected personal data, the entity shall provide the required notice prior to such collection or use, databasing, reuse, use in a learning model, or distribution, transfer, or sale.

D. Process that is due.
   1. When an individual receives notice or becomes aware that an entity subject to the provisions of this Act intends to collect, use, database, reuse, use in a learning model, distribute, transfer, or sell their personal data *prior* to that action, the individual has a right to apply to a [supreme/circuit/district/etc.] court to prevent that action and/or to ensure compliance with the provisions of this Act.
   2. Regardless of whether personal data has been lawfully or unlawfully taken or seized, an individual has a right to:
      i. Request and obtain a copy of personal data that is or was associated with, or is or was capable of being associated with, that individual from any entity subject to the provisions of this Act. The copy of personal data produced to the individual pursuant to this subsection must be disclosed both in its native format, along with any reader software or code necessary to read that native format, and in the format recommended for the data by the Library of Congress.
      ii. Correction of inaccurate personal data that is or was associated with, or is or was capable of being associated with, that individual from any entity subject to the provisions of this Act. If an entity subject to the provisions of this Act receives a request for correction, that entity must provide notice of its response to that request in accordance with the requirements of Section 3(C)(2) of this Act.
   3. When personal data is unlawfully taken or seized from an individual or unlawfully collected, used, databased, reused, used in a learning model, distributed, transferred, or sold by any entity defined in Section 1(A), that individual has a right to:
      i. Destruction, as defined in Sections 2(D) and 6(A), and
      ii. Recompense for the taking, as defined in Section 6(B).

   4. When personal data is lawfully taken or seized from an individual by or lawfully collected, used, databased, reused, used in a learning model, distributed, transferred, or sold by any entity defined in Section 1(A), that individual may have that personal data sealed:
      i. by operation of law as defined in Section 2(J) and 6(A); or
      ii. if Section 6 is inapplicable, by application to a [supreme/circuit/district/etc] court.

SECTION 4. PURPOSE AND REUSE RULES.

A. No surveillance technology may be acquired, deployed, or used without prior public notice, independent validation for reliability, and approval by an independent oversight body.

B. Each act of collection and use of personal data constitutes a separate taking and seizure of personal property for purposes of this Act.

C. Each act of data collection must satisfy standards of necessity, specificity, and proportionality. Data collection that is overbroad, untargeted, or not narrowly tailored to a lawful purpose is prohibited.

D. Unlawfully taken or seized personal data.
   1. Personal data, unlawfully taken or seized, shall not be collected or used for any purpose or in any way.
   2. Personal data, unlawfully taken or seized, shall not be reused for any purpose or in any way.
   3. Personal data, unlawfully taken or seized, shall not be databased.
   4. Learning models trained on or developed in any way from unlawfully taken or seized personal data shall not be used for any purpose or in any way.

E. Lawfully seized personal data.
   1. Personal data, lawfully taken or seized, shall only be collected and used for the specific purpose for which its collection or use was legally authorized.
   2. Personal data, lawfully taken or seized, shall not be transferred or reused, unless such transfer or reuse is specifically authorized by law.
   3. Personal data, lawfully taken or seized, shall only be databased if both the specific database and enrollment of that personal data are specifically authorized by law.
   4. Learning models shall not be trained on or developed in any way from lawfully taken or seized personal data unless specifically authorized by law.

F. No individual shall be subject to a decision of legal consequence based on automated processing or algorithmic inference. All algorithmic determinations affecting liberty or rights must be reviewable by a human decision-maker and subject to judicial scrutiny.

SECTION 5. SPECIFIC PROCEDURES FOR PERSONAL DATA IN CRIMINAL MATTERS.

A. Discovery in criminal cases.

1. Application. This Subsection governs the [City/County/State's] disclosure of material and information related to an accused's personal data in all criminal and post-conviction matters.
2. Scope of Obligations. The [City/County/State's] disclosure obligations apply to information material to the defense relating to personal data that are:
   i. In the [City/County/State's] possession or control;
   ii. In the possession or control of any corporation, non-governmental organization, or law enforcement partner that sells, distributes, or otherwise provides any of the entities listed in Section 1 with tools, technologies, or services that support law enforcement, family regulation, or corrections purposes.
   iii. These obligations explicitly include personal data of parolees, pre-trial detainees, and individuals under any form of court-ordered supervision.
   iv. Disclosure obligations shall comply with the [City/County/State's] discovery rules.
3. Due diligence. The [City/County/State] shall:
   i. Exercise due diligence to identify all material and information that must be disclosed under this Act.
   ii. Document its efforts to identify all material and information that requires disclosure under this Act.
4. State's disclosure. The [City/County/State] shall provide the following to the defense without the necessity of request:
   i. The date or date range(s) of collection, use, databasing, reuse, use in a learning model, distribution, transfer, or sale of personal data;
   ii. A description of the personal data covered under Subsection (A)(2);
   iii. The entity or entities that collected, used, databased, reused, used in a learning model, distributed, transferred, or sold personal data; and
   iv. A description of how the personal data was collected, used, databased, reused, used in a learning model, distributed, transferred, or sold.
5. Time to disclose. Disclosure under this Section shall be made at the time required under [cross-referenced Discovery Rule].
6. Continuing duty to disclose. The [City/County/State] has a continuing obligation to make disclosures pursuant to this Section. The State must promptly disclose material or information subject to disclosure under this Section that is discovered before or during trial or post-conviction proceedings.
7. Exclusion and destruction of personal data.
   i. Failure to comply. If the [City/County/State] fails to comply with the disclosure provisions of this Act, the court shall:

1. Order compliance under prescribed terms and conditions;
2. Prohibit the State from introducing the undisclosed evidence or evidence derived from it at a criminal trial or post-conviction proceeding; and
3. Reveal any undisclosed evidence derived from unlawfully taken data to the defense, whether it is incriminating or exculpatory.

ii. Destruction of Personal Data. Upon a court's finding of no probable cause, dismissal with prejudice, vacatur, finding of innocence, or acquittal, all personal data in the [City/County/State's] possession and control shall be destroyed.

B. Motions to Limit Collection, Use and Admission of Personal Data in Criminal Matters.

1. Motions to Suppress. In criminal matters, an accused person may file a motion to suppress personal data that was collected, used, databased, reused, used in a learning model, distributed, transferred, or sold in violation of this Act. Upon a showing by the accused by a preponderance of the evidence that their personal data was collected, used, databased, reused, used in a learning model, distributed, transferred, or sold in violation of this Act, such evidence and any fruits of such evidence shall be suppressed.
2. Motions seeking collection and use limitations.
   i. In general. In criminal matters, an accused person may file a motion to suppress critical categories of personal data when its collection and use, databasing, reuse, or use in a learning model burdens freedoms of speech or association and/or has a personal and/or collective chilling effect on the exercise of those freedoms.
   ii. Procedure. Upon a showing by the accused that the collection and use, databasing, reuse, or use in a learning model (1) involved a critical category or critical categories of personal data and (2) burdened freedoms of speech or association and/or had a personal and/or collective chilling effect on the exercise of the freedoms of speech or association, the burden will shift to the prosecution to establish that (1) the collection and use, databasing, reuse, or use in a learning model furthers a compelling governmental interest, and (2) the collection and use, databasing, reuse, or use in a learning model activity or activities in the case were narrowly tailored to achieve that interest.
   iii. Determination by the court. If the court finds that the collection and use, databasing, reuse, or use in a learning model (1) involved a critical category or critical categories of personal data, (2) burdened the freedoms of speech or association and/or had a personal and/or collective chilling effect on the exercise of those freedoms, and (3) did not further a compelling governmental interest or, if it did, was not narrowly tailored to achieve that interest, such evidence, along with any fruits derived from its collection and use, databasing, reuse, or use in a learning model, shall be suppressed.
3. The provisions of [cross-reference applicable rule/statue on motions to suppress] shall apply to motions to suppress made under this Section.

SECTION 6. DESTRUCTION, SEALING, AND RECOMPENSE.

A. Destruction and sealing rules.
   1. Unlawfully seized personal data shall be destroyed.
   2. Lawfully seized personal data shall be sealed by operation of law at the conclusion of the case in which the personal data was lawfully seized.
      i. In general. For purposes of this subsection, a case concludes when there is a conviction or favorable result for the defendant or, if no charges are ever brought, the case concludes when the [District Attorney] declines to prosecute, there is no investigative activity in the case for one month, or 90 days pass without an arrest, grand jury presentation, or arrest warrant being issued, whichever occurs earlier.
      ii. Procedure to reopen.
         1. Sealed personal data may not be reopened if a case concludes favorably for the accused, except upon the request of the accused.
         2. If a conviction is obtained and the personal data in the case is sealed, any entity defined in Section 1(A) may only request access to sealed data from a court of competent jurisdiction and only in connection with a formally reopened case on appeal or other authorized legal proceeding.
         3. Upon a showing by clear and convincing evidence that any entity defined in Section 1(A) requires access to the sealed data in order to prosecute a newly ordered trial or post-conviction hearing, the court may authorize access to sealed data for that limited purpose only.
   3. Any database, not specifically authorized by law, that databases personal data shall be destroyed.
   4. Learning models trained on or developed in any way from unlawfully seized personal data shall be destroyed.
   5. Learning models trained on or developed in any way from lawfully seized personal data, unless specifically authorized by law, shall be destroyed.

B. Private right of action. Any person aggrieved by a violation of this Act shall have a right of action in a State [supreme/circuit/district/etc.] court or as a supplemental claim in federal district court against an offending party. A prevailing party may recover for each violation:
   1. Against an entity described in Section 1 that negligently violates a provision of this Act, liquidated damages of [____] or actual damages, whichever is greater;
   2. Against an entity described in Section 1 that intentionally or recklessly violates a provision of this Act, liquidated damages of [____] or actual damages, whichever is greater;
   3. Punitive damages in appropriate cases;
   4. Reasonable attorneys' fees and costs, including expert witness fees and other litigation expenses; and
   5. Other relief, including an injunction, as the [City/County/State] or federal court may deem appropriate.

ENDNOTES

1 GEORGE ORWELL, NINETEEN EIGHTY-FOUR 3 (1949).

2 DANIEL J. SOLOVE, ON PRIVACY AND TECHNOLOGY 18 (Oxford Univ. Press 2025). Professor Daniel Solove describes how many privacy harms resemble the experience of being subjected to an incomprehensible and unaccountable bureaucratic system, rather than direct authoritarian coercion. *Id.* In *The Trial*, Franz Kafka depicts an ordinary man entangled in a faceless legal bureaucracy whose rules are unknowable and whose decisions are unchallengeable. *Id.* Solove uses this analogy to illustrate how modern data systems create confusion, powerlessness, and lack of recourse. *Id.*

3. VIRGINIA EUBANKS, AUTOMATING INEQUALITY: HOW HIGH-TECH TOOLS PROFILE, POLICE, AND PUNISH THE POOR 6 (St. Martin's Press 2018).

4. *Id.*

5. *See* VIKTOR MAYER-SCHÖNBERGER & KENNETH CUKIER, BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK 78 (Houghton Mifflin Harcourt 2013) (coining the term "datafication" and defining datafication as putting something "in quantified format so it can be tabulated and analyzed.").

6. 597 U.S. 215 (2022).

7. Barry Friedman & Danielle Keats Citron, *Indiscriminate Data Surveillance*, 110 VA. L. REV. 1351, 1354–55 (2024) (describing post-*Dobbs* concerns about the use of menstrual tracking data in criminal investigations and noting that such fears are "entirely justifiable").

8. *Id.* at 1355 ("At volume, all data becomes intimate data, and today, law enforcement is gathering it up by the terabyte. On each and every one of us.").

9. *Id.* at 1362–63 (warning that broad government access to intimate digital traces "is a prescription for tyranny" and of the risk that government can "pry into our virtual and physical bedrooms and bathrooms").

10. Daniel J. Solove, *"I've Got Nothing to Hide" and Other Misunderstandings of Privacy*, 44 SAN DIEGO L. REV. 745, 756–57 (2007).

11. 18 U.S.C. §§ 2701–2713.

12. *E.g.*, Ill. Biometric Information Privacy Act, 740 Ill. Comp. Stat. 14/1 et seq. (prohibiting collection and use of biometric identifiers without informed consent); California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.100 et seq.; California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.100 et seq.; California Online Privacy Protection Act (CalOPPA), Cal. Bus. & Prof. Code § 22575 et seq.; Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996).

13. Chris Gelardi, *More Than 5,000 People Are on a NY State Police Gang Database That's Talking to ICE*, THE CITY (Apr. 24, 2025), https://www.thecity.nyc/2025/04/24/gang-database-new-york-trump-immigration-enforcement/; *see also* Elizabeth Daniel Vasquez, *The N.Y.P.D. Is Teaching America How to Track Everyone Every Day Forever*, N.Y. TIMES (Sept. 15, 2025), https://www.nytimes.com/interactive/2025/09/15/opinion/nypd-surveillance.html (providing a compilation of how these forms of data collection, analysis, and sorting shape our daily lives).

14. Gelardi, *supra* note 13.

15. *Id.*

16. Julia Poe, *A Chicago Bulls Hat Triggered a Man's Deportation — and Profiling of Such Apparel and Tattoos Could Be on the Rise*, CHI. TRIB. (Apr. 11, 2025, updated Apr. 12, 2025), https://www.chicagotribune.com/2025/04/11/chicago-bulls-apparel-trump-ice-detainments/.

17. *Id.*

18. *Spying on Protesters*, ACLU, https://www.aclu.org/issues/free-speech/rights-protesters/spying-protesters (last visited Nov. 20, 2025).

19. Ivey Dyson, José Guillermo Gutiérrez & Yeshi Milner, *Records Show DC and Federal Law Enforcement Sharing Surveillance Info on Racial Justice Protests*, BRENNAN CTR. FOR JUST. (May 15, 2024), https://www.brennancenter.org/our-work/analysis-opinion/records-show-dc-and-federal-law-enforcement-sharing-surveillance-info.

20. *See* Vincent M. 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. 2, 17–23 (2023) (cataloging the myriad ways police have historically weaponized and continue to weaponize surveillance against communities of color and how innovations in surveillance technologies have exacerbated racial harms).

21. *See* EXEC. OFF. OF THE PRESIDENT, BIG DATA: A REPORT ON ALGORITHMIC SYSTEMS, OPPORTUNITY, AND CIVIL RIGHTS 4–6 (2016) (explaining that algorithmic systems can "perpetuate, exacerbate, or mask" discriminatory harms through biased data inputs and design choices).

22. *See* Peter A. Chow-White & Troy Duster, *Do Health and Forensic DNA Databases Increase Racial Disparities?*, 8 PLOS MED. 1, 2 (2011) (explaining that racial disparities in policing and incarceration are reproduced In forensic DNA databases and that these systems disproportionately contain the DNA of Black and Latino individuals); Duncan Purves, *Fairness in Algorithmic Policing*, 8 J. AM. PHIL. ASS'N 741, 745–49 (2022), https://philpapers.org/rec/PURFIA (explaining how predictive policing systems can generate self-reinforcing feedback loops that concentrate police attention in Black communities and disproportionately burden innocent residents through heightened surveillance and enforcement).

23. *See*, *e.g.*, Kashmir Hill, *Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match*, N.Y. TIMES (Dec. 29, 2020, updated Jan. 6, 2021), https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html (reporting multiple wrongful arrests caused by erroneous facial recognition matches, including a man jailed for days after a misidentification); Katherine Jeng, *Wrongful Convictions Revealed the Dangers of Trusting Unvalidated Science. Are We About to Repeat the Same Mistakes with AI?*, INNOCENCE PROJECT (Oct. 3, 2024), https://innocenceproject.org/news/wrongful-convictions-revealed-the-dangers-of-trusting-unvalidated-science-are-we-about-to-repeat-the-same-mistakes-with-ai/ (explaining that unvalidated forensic and AI-driven tools have contributed to wrongful convictions and warning of renewed risks as police adopt opaque AI systems); CLARE GARVIE & LAURA M. MOY, AMERICA UNDER WATCH: FACE SURVEILLANCE IN THE UNITED STATES, GEO. L. CTR. ON PRIV. & TECH. (May 16, 2019), https://www.americaunderwatch.com/ (documenting widespread police use of real-time face surveillance systems that enable misidentifications, expand discretionary police power, and heighten risks of discriminatory and violent encounters).

24. Chaz Arnett, *Data, the New Cotton*, JUST TECH. SOC. SCI. RSCH. COUNCIL (May 25, 2022), https://doi.org/10.35650/JT.3034.d.2022.

25. *Id.*

26. Carpenter v. United States, 585 U.S. 296, 311 (2018).

27. *See* Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting) (describing the "right to be let alone" as the "most valued" right, a formulation that has since become foundational to constitutional conceptions of privacy).

28. *See*, *e.g.*, Barry Friedman, *The Constitutionality of Indiscriminate Data Surveillance*, U. PA. L. REV. (forthcoming 2026) (manuscript at 2) (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5164756) ("No court should even consider upholding indiscriminate data surveillance until such a policy [regulating data surveillance]—preferably legislatively authorized—is in place"); Mary F. Fan, *Suspecting With Data*, 109 MINN. L. REV. 2253, 2257 (2025) ("[T]his article advances beyond Fourth Amendment fetishism and stalemates, and theorizes why evidence law protections and procedures are better suited to address the concerns posed by such big data search strategies."); Maneka Sinha, *The Automated Fourth Amendment*, 73 EMORY L.J. 589, 651–53 (2024) (contending that constitutional doctrine alone cannot constrain government use of automated technology and urging statutory intervention to close resulting privacy gaps); BRENNAN CTR. FOR JUST., THE PUBLIC OVERSIGHT OF SURVEILLANCE TECHNOLOGY (POST) ACT: A RESOURCE PAGE (June 12, 2017), https://www.brennancenter.org/our-work/research-reports/public-oversight-surveillance-technology-post-act-resource-page (describing New York City's Public Oversight of Surveillance Technology Act, which requires the NYPD to disclose, evaluate, and obtain public and legislative approval for its use of surveillance technologies, and documenting advocacy by community organizations and civil liberties groups for statutory transparency and oversight).

29. *See* Friedman & Citron, *supra* note 7, at 1378–80 (explaining that the Privacy Act's law enforcement exemptions permit agencies to exempt entire databases from core protections and noting that Congress anticipated follow-on legislation regulating criminal justice databases that was never enacted).

30. *See* Tracey L. Meares, *Policing and Procedural Justice: Shaping Citizens' Identities to Increase Democratic Participation*, 111 NW. U. L. REV. 1525, 1530–32 (2017) (explaining the social psychological foundations of procedural justice and how perceived fairness shapes legitimacy).

31. Monica C. Bell, *Police Reform and the Dismantling of Legal Estrangement*, 126 YALE L.J. 2054, 2066–69 (2017).

32. *See* United States v. Jones, 565 U.S. 400, 415–16 (2012) (Sotomayor, J., concurring) (warning that long-term, aggregated surveillance permits the government to "ascertain, more or less at will, [a person's] political and religious beliefs, sexual habits, and so on," and describing how comprehensive monitoring reveals "a wealth of detail about [a person's] familial, political, professional, religious, and sexual associations"); *Carpenter*, 585 U.S. at 310–11 (reasoning that access to seven days of historical cell-site location information reveals the whole of a person's physical movements, enabling retrospective tracking, exposure of familial, political, professional, religious, and sexual associations, and reconstruction of the privacies of life).

33. Khari Johnson, *How Wrongful Arrests Based on AI Derailed 3 Men's Lives*, WIRED (Mar. 7, 2022), https://www.wired.com/story/wrongful-arrests-ai-derailed-3-mens-lives/. This article also includes several other examples, including Robert Williams, who was arrested in front of his family in Michigan based on a faulty facial recognition match, detained for 30 hours, and continues to suffer lasting harm. His young daughter remains traumatized, and he has suffered multiple strokes since the incident. Similarly, Michael Oliver lost his job as a car-parts painter after being wrongfully accused of larceny when Detroit police relied on a blurry screenshot that facial recognition erroneously identified as a portrait of him.

34. *Id.*

35. Michael Pinard, *Collateral Consequences of Criminal Convictions: Confronting Issues of Race and Dignity*, 85 N.Y.U. L. REV. 457, 459–60, 470 (2010).

36. Johnson, *supra* note 33.

37. Friedman & Citron, *supra* note 7, at 1357 (warning that mass data surveillance "has made suspects of us all" by exposing people to investigative scrutiny without individualized suspicion).

38. *See* SARAH BRAYNE, PREDICT AND SURVEIL: DATA, DISCRETION, AND THE FUTURE OF POLICING, 52–55 (2021) (defining "dragnet surveillance" as ongoing, programmatic, and automated data collection that expands the universe of people subject to police scrutiny).

39. *Id.* at 9–11.

40. *See* Chow-White & Duster, *supra* note 22, at 2; Erin Murphy & Jun H. Tong, *The Racial Composition of Forensic DNA Databases*, 108 CALIF. L. REV. 1847, 1847–52, 1894–99 (2020).

41. Grace Burke, Juliet Linderman, Martha Mendoza & Michael Tarm, *How AI-Powered Tech Landed Man in Jail With Scant Evidence*, AP NEWS (Mar. 5, 2022), https://apnews.com/article/artificial-intelligence-algorithm-technology-police-crime-7e3345485aa668c97606d4b54f9b6220.

42. Joseph Cox, *Candy Crush, Tinder, MyFitnessPal: See the Thousands of Apps Hijacked to Spy on Your Location*, WIRED (Jan. 9, 2025), https://www.wired.com/story/gravy-location-data-app-leak-rtb/.

43. Raisa Bruner, *Man Arrested in Wife's Murder After Fitbit Data Pokes Holes in His Alibis*, TIME (Apr. 25, 2017), https://time.com/4755137/fitbit-murder-alibi-richard-connie-dabate/.

44. *See* Haeyoung Chung, Shinelle Hutchinson, Umit Karabiyik, Mohammad Meraj Mirza, Tathagata Mukerjee, Carrie Pettus-Davis, Marcus K. Rogers & Nicholas West, *Investigating Wearable Fitness Applications: Data Privacy and Digital Forensics Analysis on Android*, 12 APPLIED SCI. 9747, 9748–49 (2022), https://doi.org/10.3390/app12199747 (documenting that data extracted from wearable devices, including step counts, GPS traces, timestamps, and heart-rate logs, have been used in criminal investigations and can support timeline reconstruction).

45. Sally Ho & Jason Dearen, *Child Welfare Algorithm Faces Justice Department Scrutiny*, AP NEWS (Mar. 15, 2023), https://apnews.com/article/4f61f45bfc3245fd2556e886c2da988b (describing Department of Justice Civil Rights Division investigation into Allegheny County's predictive child welfare algorithm).

46. *See* Anjana Samant, Aaron Horowitz, Kath Xu, and Sophie Beiers, *Family Surveillance by Algorithm: The Rapidly Spreading Tools Few Have Heard Of*, ACLU (Sept. 29, 2021), https://www.aclu.org/documents/family-surveillance-algorithm (describing how predictive analytics tools built from historical data can lead to disproportionate system contact for families in disadvantaged communities).

47. *See* Rashida Richardson, Jason M. Schultz & Kate Crawford, *Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice*, 94 N.Y.U. L. REV. 15, 40–48 (2019) (arguing that predictive policing systems trained on "dirty data" derived from unlawful or biased police practices reproduce and reinforce those same injustices through feedback loops).

48. Kristen Lum & William Isaac, *To Predict and Serve?*, 13 SIGNIFICANCE 14, 15–19 (2016).

49. *Id.* at 15–16.

50. *See* Danielle Ensign, Sorelle A. Friedler, Scott Neville, Carlos Scheidegger & Suresh Venkatasubramanian, *Runaway Feedback Loops in Predictive Policing*, 81 PROC. MACH. LEARNING RES. 1, 1–5 (2018) (demonstrating mathematically that minimal initial differences in enforcement generate allocation disparities over time).

51. *See*, *e.g.*, RUHA BENJAMIN, RACE AFTER TECHNOLOGY: ABOLITIONIST TOOLS FOR THE NEW JIM CODE 12–15 (2019) (explaining how ostensibly neutral technologies inherit and reproduce racial hierarchies under the guise of technical objectivity); EUBANKS, *supra* note 3, at 6–7 (arguing that data systems mirror and reinforce structural inequities in welfare, criminal justice, and public services); SAFIYA UMOJA NOBLE, ALGORITHMS OF OPPRESSION: HOW SEARCH ENGINES REINFORCE RACISM 1–3, 12–14 (2018) (explaining that algorithmic systems inherit and normalize biased cultural representations, reinforcing existing hierarchies while appearing neutral).

52. *See* Richardson et al., *supra* note 47, at 198–204 (explaining how data drawn from discriminatory practices broadens police datasets and compounds racial inequity); *see also* BRAYNE, *supra* note 38, at 63–66 (describing how dragnet-style data capture incorporates people with no direct police contact into law enforcement systems).

53. *See* BRAYNE, *supra* note 38, at 51–53 (explaining that in big data policing systems "queries themselves are becoming data," that systems compare similar queries across analysts to generate associative inferences, and that query counts function as "quantified proxies for suspiciousness" that can entrench feedback loops); ANDREW GUTHRIE FERGUSON, THE RISE OF BIG DATA POLICING: SURVEILLANCE, RACE, AND THE FUTURE OF LAW ENFORCEMENT 112–13, 118–22 (2017) (describing how metadata analysis and network-mapping techniques can treat incidental or out-of-context digital connections as indicators of risk and expand suspicion through associative inference).

54. The National Institute of Standards and Technology (NIST) AI Risk Management Framework defines an AI system as "an engineered or machine-based system that can, for a given set of objectives, generate outputs such as predictions, recommendations, or decisions influencing real or virtual environments." NAT'L INST. OF STANDARDS & TECH., ARTIFICIAL INTELLIGENCE RISK MANAGEMENT FRAMEWORK (AI RMF 1.0) 1 (2023), https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf. *See also* Aruna Pattam, *Artificial Intelligence, Defined in Simple Terms*, HCLTECH (Sept. 16, 2021), https://www.hcltech.com/blogs/artificial-intelligence-defined-simple-terms ("Artificial intelligence is the science of making machines that can think like humans. It can do things that are considered 'smart.' AI technology can process large amounts of data sets in ways that are unlike humans. The goal for AI is to be able to do things such as recognize patterns, make decisions and judge like humans. To do this, we need lots of data and data sets incorporated into them.").

55. *See*, *e.g.*, Jenne Burrell, *How the Machine 'Thinks': Understanding Opacity in Machine Learning Algorithms*, 3 BIG DATA & SOC'Y (Special Issue) 1 (2016) (describing how machine learning systems obscure their internal reasoning, creating a black box problem).

56. BRAYNE, *supra* note 38, at 43–44, 55–56.

57. *Id.*

58. *Id.* at 51–53.

59. *Id.* at 64–67, 74–76.

60. Olmstead v. United States, 277 U.S. 438, 478–79 (1928) (Brandeis, J., dissenting).

61. *Id.* at 478.

62. *See* Carpenter v. United States, 585 U.S. 296, 320 (2018) (emphasizing that the Fourth Amendment protects privacy beyond physical intrusion).

63. *Id.* at 310.

64. *Id.* at 297.

65. Elizabeth E. Joh, *The New Surveillance Discretion: Automated Suspicion, Big Data, and Policing*, 10 HARV. L. & POL'Y REV. 15, 27–29 (2016).

66. The proposed data deletion procedure is consistent with the "right to erasure" under the General Data Protection Regulation. Regulation 2016/679, art. 17, 2016 O.J. (L 119) 33 (EU), available at https://gdpr-info.eu/art-17-gdpr/.

67. *Id.*

68. *See generally* Steven Aftergood, *The Fourth Amendment Third-Party Doctrine, & More from CRS*, FED'N OF AM. SCIENTISTS (June 12, 2014), https://fas.org/publication/third-party/ ("People who voluntarily share information with a third party are not entitled to an expectation of privacy concerning that information under the so-called 'third-party doctrine' that currently prevails in judicial interpretations of the Fourth Amendment to the Constitution.").

69. *See* Niva Elkin-Koren & Michal S. Gal, *The Chilling Effect of Governance-by-Data on Data Markets*, 86 U. CHI. L. REV. 403, 424 (2019) ("[I]n some situations nonuse is not an option or could be extremely costly.").

70. Andrea Roth, *"Spit and Acquit": Prosecutors as Surveillance Entrepreneurs*, 107 CALIF. L. REV. 405, 408 (2019).

71. *See* Kay L. Levine, Jonathan Remy Nash & Robert A. Schapiro, *The Unconstitutional Conditions Vacuum in Criminal Procedure*, 133 YALE L.J. 1401, 1412, 1482 (2024) (arguing that the unconstitutional conditions doctrine should apply in the criminal procedure context).

72. *Id.*

73. *See* Kate Weisburd, *Sentenced to Surveillance: Fourth Amendment Limits on Electronic Monitoring*, 98 N.C. L. REV. 717, 740 (2020) (noting that individuals' consent to electronic monitoring or search conditions is often neither fully "knowing" nor truly voluntary, and that such conditions frequently operate as "add-ons" rather than negotiated trade-offs for reduced punishment).

74. *See* EUBANKS, *supra* note 3, at 12 (describing how "[a]utomated decision-making shatters the social safety net, criminalizes the poor, intensifies discrimination, and compromises our deepest national values.").

75. Drew Harwell, *Federal Study Confirms Racial Bias of Many Facial-Recognition Systems, Casts Doubt on Their Expanding Use*, WASH. POST (Dec. 19, 2019), https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/.

76. *See* N.Y. CIVIL LIBERTIES UNION, THE PROBLEMS WITH PRETRIAL RISK ASSESSMENT TOOLS 3 (2020), https://www.nyclu.org/uploads/2020/03/20200309_bailriskassessment_v3.pdf.

77. EMBER MCCOY, THE RISKS OF PRETRIAL RISK ASSESSMENT TOOLS: POLICY CONSIDERATIONS FOR MICHIGAN 5, (Sci., Tech. & Pub. Pol'y (STPP), Ford Sch. of Pub. Pol'y., 2023), https://stpp.fordschool.umich.edu/sites/stpp/files/2023-05/Risk%20Assessment%20Policy%20Brief%20Final%205.2.23_0.pdf.

78. *See* Stacy-Ann Elvy, *Paying for Privacy and the Personal Data Economy*, 117 COLUM. L. REV. 1369, 1376–77, 1379–80, 1390–91 (2017) (describing personal data's economic commodification and transferability in the personal data economy).

79. Ensuring Likeness, Voice, and Image Security Act, 2024 Tenn. Pub. Ch. 588, codified at TENN. CODE ANN. § 47-25-1101–1106.

80. Emile Ayoub & Elizabeth Goitein, *Closing the Data Broker Loophole*, BRENNAN CTR. FOR JUST. (Feb. 13, 2024), https://www.brennancenter.org/our-work/research-reports/closing-data-broker-loophole.

81. Joseph Cox, *How the U.S. Military Buys Location Data from Ordinary Apps*, VICE (Nov. 16, 2020), https://www.vice.com/en/article/us-military-location-data-xmode-locate-x.

82. *See* James Grimmelmann & Christina Mulligan, *Data Property*, 72 AM. U. L. REV. 829, 883 (2022) (arguing that modern life depends as heavily on digital objects as on physical ones and that "data is property" within existing personal property doctrine and explaining that their framework situates data alongside other intangible but legally protectable interests and that recognizing data as property need not create a sweeping new intellectual property regime, but instead restores coherence to how the law treats assets people rely on every day). *See also* Pamela Samuelson, *Privacy as Intellectual Property*, 52 STAN. L. REV. 1125, 1139–41 (2000) (exploring privacy and personal data interests through an intellectual property framework and highlighting the ways personal data implicates reputational, autonomy, and personal interests typically associated with rights in creative works).

83. *See* Samuelson, *supra* note 82, at 1135–36 (explaining that U.S. law frequently recognizes protectable interests in information through doctrines like unfair competition, confidential relationships, and database protection and that Congress has a historically created property-like rights in information to correct market failures or promote socially valuable production).

84. *Compare* Jeffrey Ritter & Anna Mayer, *Regulating Data as Property: A New Construct for Moving Forward*, 16 DUKE L. & TECH. REV. 220, 223 (2018) (proposing a property rights framework for data), *with* Cameron F. Kerry & John B. Morris, *Why Data Ownership Is the Wrong Approach to Protecting Privacy*, BROOKINGS INST. (June 26, 2019), https://www.brookings.edu/articles/why-data-ownership-is-the-wrong-approach-to-protecting-privacy/ (arguing that data ownership frameworks do not effectively protect privacy).

85. Jacob M. Victor, Comment, *The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy*, 123 YALE L.J. 513, 516 (2013).

86. Fuentes v. Shevin, 407 U.S. 67, 80 (1972).

87. *See*, *e.g.*, Bennett Cyphers, *How the Federal Government Buys Our Cell Phone Location Data*, ELEC. FRONTIER FOUND. (June 13, 2022), https://www.eff.org/deeplinks/2022/06/how-federal-government-buys-our-cell-phone-location-data (explaining that federal agencies purchase location data harvested from consumer apps and repurpose it for law enforcement and intelligence investigations without adhering to traditional warrant requirements); Shreya Tewari & Fikayo Walter-Johnson, *New Records Detail DHS Purchase and Use of Vast Quantities of Cell Phone Location Data*, ACLU (July 18, 2022), https://www.aclu.org/news/privacy-technology/

new-records-detail-dhs-purchase-and-use-of-vast-quantities-of-cell-phone-location-data (reporting that U.S. Customs and Border Protection and U.S. Immigration and Customs Enforcement obtained commercially collected location data originally gathered for advertising and analytics and used it in immigration and criminal investigations); OFF. OF INSPECTOR GEN., U.S. DEP'T OF HOMELAND SEC., CPB, ICE, AND SECRET SERVICE DID NOT ADHERE TO PRIVACY POLICIES OR DEVELOP SUFFICIENT POLICIES BEFORE PROCURING AND USING COMMERCIAL TELEMETRY DATA (REDACTED) OIG-23-61 4 (2023), https://www.oig.dhs.gov/sites/default/files/assets/2023-09/OIG-23-61-Sep23-Redacted.pdf (finding that various U.S. agencies did not develop or follow policies prior to obtaining and using commercial telemetry data).

88. *See* Cox, *supra* note 42.

89. Douglas MacMillan, David Ovalle & Aaron Schaffer, *Arrested by AI: Police Ignore Standards After Facial Recognition Matches*, WASH. POST. (Jan. 13, 2025), https://www.washingtonpost.com/business/interactive/2025/police-artificial-intelligence-facial-recognition/.

90. *Id.*

91. *See* Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993) (establishing that trial judges must act as gatekeepers and admit only scientific evidence that is reliable and relevant).

92. *See* Christopher Lau, *Shadow Forensics: Uncovering 911 Call Analysis*, 111 CORNELL L. REV. (forthcoming 2026) (manuscript at 24–25) (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5164732) (describing how prosecutors fail to disclose use of surveillance technology and forensic methods, and as a result, such tools "escape evidentiary examination[.]").

93. CLARE GARVIE, A FORENSIC WITHOUT THE SCIENCE: FACE RECOGNITION IN U.S. CRIMINAL INVESTIGATIONS, GEO. L. CTR. ON PRIV. & TECH. 20 (2022), https://mcusercontent.com/672aa4fbde-73b1a49df5cf61f/files/2c2dd6de-d325-335d-5d4e-84066159df71/Forensic_Without_the_Science_Face_Recognition_in_U.S._Criminal_Investigations.pdf (critiquing the fact that "[t]here is no national level law, regulation or policy requiring the companies that sell face recognition algorithms or the law enforcement agencies that purchase them to submit the algorithm to an independent accuracy test, and no law or federal regulatory standard exists prescribing minimum accuracy thresholds.").

94. Fan, *supra* note 28, at 2254, 2319–20, 2323–25.

95. *See Id.* at 2287 ("[U]nderstanding the comparatively greater constraints on law enforcement agencies compared to businesses in gathering and using data illuminates the grave concerns with using privately collected and controlled data as a basis for identifying suspects and justifying stops, arrests, and convictions.").

96. *Id.* at 2288; *see also* Rebecca Wexler, *Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System*, 70 STAN. L. REV. 1343, 1354, 1358–68 (2018) (detailing how vendors invoke trade secret and copyright protections to avoid disclosing source code, validation data, and error rates, arguing that disclosure would jeopardize competitive advantage and reveal proprietary methods).

97. *See* Fan, *supra* note 28, at 2288 (describing how IP laws protect private developers against independent scrutiny and even law enforcement agencies that contract with them can be contractually bound to non-disclosure agreements); Hannah Bloch-Wehba, *Access to Algorithms*, 88 FORDHAM L. REV. 1265, 1272 (2020) (describing how access to government records is routinely frustrated because agencies procure algorithmic tools through contracts that include sweeping protections for trade secrets and proprietary information, thereby legally insulating these systems from public oversight). Additionally, trade secret protections have created barriers to transparency in forensic DNA analysis, with courts in several states denying defense access to proprietary source code for probabilistic genotyping software, though some jurisdictions have ordered disclosure under protective orders to balance accused persons' rights against commercial interests. Fan, *supra* note 28, at 2289.

98. *See* Southerland, *supra* note 20, at 60–73 (outlining challenges to establishing meaningful community authority over law enforcement surveillance technology).

99. *See* EXEC. OFF. OF THE PRESIDENT, *supra* note 21, at 5 (noting that improperly implemented big data technologies can "perpetuate, exacerbate, or mask harmful discrimination.").

100. *See supra* notes 18–25 and accompanying text (highlighting the potential for everyday data collection to be used in ways that affect privacy and civil liberties and target marginalized populations).

101. *See* Southerland, *supra* note 20, at 17–23 (cataloging the ways police have historically weaponized and continue to weaponize surveillance against communities of color).

102. *Id.* at 23–24 (describing how constant surveillance "contributes to a collective sense of procedural injustice" and can exacerbate "structural exclusion").

103. *See supra* notes 7–9 and accompanying text (discussing how data collected for routine or administrative purposes, including reproductive health data, can later be repurposed by law enforcement and other actors when political or legal conditions change).

104. *See supra* notes 46–51 and accompanying text (explaining how data and data sets reflect societal disparities).

105. *See* Chow-White & Duster, *supra* note 22, at 2 (observing that racial inequities in policing and incarceration are reflected in forensic DNA databases).