# BIG DATA: GUISING AND FUNCTIONALLY CREEPING TOWARD CIVIL DEATH

*RAYMOND TRENT CROMARTIE**

TABLE OF CONTENTS



## I.
## INTRODUCTION

Civil death, a concept that was once borrowed from English common law (the antecedent to our own legal system), has steadily eroded since the 1800s.[1] At its core, civil death was a punishment that extinguished the civil rights of any individual found responsible for a crime or other wrongdoing.[2] Once attached, this stigma impacted an individual's ability to maintain property, pursue legal claims, perform any legal function, and vote, among many other things.[3]

---

* To my friends, family, and loved ones, thank you. Without your support, I would not be here today.

1. *See generally* Gabriel J. Chin, *The New Civil Death: Rethinking Punishment in the Era of Mass Conviction*, 160 U. Pa. L. Rev. 1789, 1793–1815 (2012) ("By the turn of the nineteenth century, civil death faced increasingly withering criticism.").

2. *See id.* at 1790 ("Civil death extinguished most civil rights of a person convicted of a crime and largely put that person outside the law's protection."); *see also* Harry David Saunders, *Civil Death—A New Look at an Ancient Doctrine*, 11 Wm. & Mary L. Rev. 988, 989 (1970) (describing an 1888 New York court decision that held a convict could no longer perform legal functions).

3. *See* Alec C. Ewald, *"Civil Death": The Ideological Paradox of Criminal Disenfranchisement Law in the United States*, 2002 Wis. L. Rev. 1045, 1049 n. 13 (2022) ("The term 'civil death' refers to the condition in which a convicted offender loses all political, civil, and legal rights.").

Although the reliance upon civil death steadily declined in the 1900s and has seemingly disappeared in our legal system, it can be argued that it has simply undergone metamorphosis and modernization. Where colonial legal processes publicly sentenced individuals to a civil death, our current system, through the use of unrecognized technological processes to further public safety, now exacerbates the impact of existing collateral consequences. Such consequences have generally been defined as secondary impacts of a criminal conviction or civil judgment.[4] The result of this is an environment that may facilitate a civil death for anyone found responsible of criminal or civil stigma. While collateral consequences may not be inherently tied to a conviction or judgment,[5] they certainly arise after the legal finding and can have a substantial impact on one's ability to live and pursue basic civil rights.[6] Depending upon the nature of a conviction, judgment, or finding of responsibility, a collateral consequence may affect one's ability to obtain employment, vote, purchase a firearm, maintain housing, qualify for government benefits, and pursue an education, among many other things.[7]

The current effect of collateral consequences is amplified by the fact that law enforcement in our society now maintains digital forms of recordkeeping or data processing that allows an untold number of individuals and entities to access databanks that may house information about millions of citizens. Such data stores may even include information about individuals who have no criminal record or other history of wrongdoing, potentially resulting in a negative stigma being attached to someone without any due process or other constitutional safeguards triggering. As discussed in greater detail below, the nature and substance of the aforementioned information collected and stored by law enforcement entities can have significant, long-lasting impacts on individuals, depending upon what information is collected, how it is used, and who is using it.

---

4. *See* Jenny Roberts, *Expunging America's Rap Sheet in the Information Age*, 2015 Wis. L. Rev. 321, 327 (2015) ("Collateral consequences are the purportedly non-punitive, noncriminal consequences that can flow automatically or as a matter of discretion from a criminal conviction.").

5. As addressed below, the use of big data can impose collateral consequences on individuals even if they have no police contact or criminal or civil record. *See infra* Part II.

6. *See* Roberts, *supra* note 4, at 327 ("These consequences affect a person's employment and housing prospects, parental rights, educational opportunities, freedom of movement, and just about every other aspect of daily life.").

7. *What are Collateral Consequences?*, Nat'l Inventory of Collateral Consequences of Conviction, https://niccc.nationalreentryresourcecenter.org/ [https://perma.cc/2VN7-U246] (last visited Sep. 4, 2025).

Criminal recordkeeping and collateral consequences have been present in the United States for decades and have been a focus of civil discourse for just as long.[8] While one side touts the use of criminal recordkeeping as a hallmark of public safety and efficiency,[9] other advocates highlight the significant negative impact of collateral consequences. The effect and severity of any consequence has been heightened by the rapid transition from paper recordkeeping to digital, as well as the corresponding development of related technology.[10] Where court systems or other government entities were once the only place to harbor information regarding an individual's criminal or civil background, records are now being acquired through ever-expanding means and uploaded into massive databases or other technological processes that can be readily accessed by an unknown number of parties.[11] For example, since this move to digital storage, private companies and individuals have capitalized on the opportunity by amassing and selling private information, thereby increasing exposure for anyone whose information is housed within these databases.[12] Compounding this issue is the free flow of information exchange in today's society, which occurs in milliseconds and at a global scale. Oftentimes, once an individual's information is placed

8. As a preliminary matter, the term "criminal record" traditionally refers to information that government actors maintain about an individual's criminal background or history of wrongdoing. For purposes of this Article, I expand that definition to refer to any piece of information that law enforcement has collected and stored in big data because it informs how law enforcement entities and other actors perceive individuals and how law enforcement performs its functions.

9. *See* Cynthia Diane Stephens, *Keeping an Arrest from Resulting in a Life Sentence*, MICH. BAR J., Nov. 2008, at 29, 31 ("The most potent argument for broad access to criminal history data is to preserve public safety. The right to a safe and peaceful environment is a core value for a civilized society, and employers cannot allow known dangers in the workplace.").

10. *See* Roberts, *supra* note 4, at 341 ("Once information is released, it is disseminated into the digital world in so many potential venues that a person can never fully 'expunge' anything.").

11. *See id.* ("While an expunged or sealed conviction will not show up in a public search of an official court database, a background checking company may have gathered the data before the expungement and failed to update it afterwards.").

12. *See* Caleb Brennan, *Background Check Industry Profits Off 'Digital Punishment,' Despite Flawed Data*, THE APPEAL (Apr. 17, 2023), https://theappeal.org/criminal-background-checks-industry-for-profit/ [https://perma.cc/S44N-DVSB] ("Over the past two decades, the widespread public availability of criminal records and court documents has helped fuel a global, for-profit background check industry worth billions. . . . But their assessments are often deeply flawed, in part because background check companies tend to rely on the cheapest and most easily accessible data, which is also the most prone to inaccuracies. The growth of this industry has given rise to new forms of 'digital punishment' . . . .").

on the Internet or within a database, it may be indefinitely available and may never be fully expunged.[13] These large data stores and rapid technological recordkeeping processes are generally known as "big data," a term referring to incredibly large indexing systems that house information, and these systems continue to grow exponentially as more data is input over time.[14] However, for purposes of this Article, I use the term "big data" to focus on how information flows, rather than the size of these data stores.

I recently learned of a civil protection matter where an individual was seeking a restraining order against her ex-partner, who had been alleged to be abusive. Through their own research, counsel for the petitioner, the party seeking the protection order, discovered a privately maintained database on the Internet that contained certain criminal records on individuals who had been accused of domestic violence. Unbeknownst to the respondent, the party facing the protection order, the database contained an expunged record from a prior criminal matter that was never removed or updated in the system. Counsel for petitioner sought to introduce this data at trial and, after lengthy argument, the court ultimately admitted it into evidence.[15] The primary issue in this scenario is that an *expunged* criminal record was publicly available on the Internet for anyone to review. The respondent in this matter had no idea the information existed publicly and was not aware of that fact until he was a party to a legal proceeding. Ultimately, the expunged record led to the respondent losing at trial and a permanent protection order being entered. As discussed in greater detail below, these scenarios are becoming increasingly frequent and are a clear example of how big data can have long-lasting impacts on one's life if we do not exercise due care. Due to an inaccurate, privately operated database, an expungement that may

13. *See* Meg Leta Ambrose, Nicole Friess & Jill Van Matre, *Seeking Digital Redemption: The Future of Forgiveness in the Internet Age*, 29 Santa Clara High Tech. L. J. 99, 104 (2012) ("Advances in computer storage, content distribution, and information filtering have created ubiquitous information networks that threaten one's ability to make mistakes without . . . a mark on one's permanent record, aggregated and presented to anyone by Google."); *see also id.* at 111 ("Assuming information remains indefinitely accessible to a search engine, 'forgiving' anyone, including oneself, may be incredibly problematic. The perpetual memory of the Internet hinders forgetting, thereby stifling forgiveness. 'Online, the past remains fresh. The pixels do not fade with time as our memories do.'").

14. *See generally* Bernard Marr, *What is Big Data?*, Bernard Marr & Co., https://bernardmarr.com/what-is-big-data/ [https://perma.cc/Z28S-AXY5] (last visited Sept. 4, 2025).

15. Since litigants in civil protection disputes are protected in Colorado, the identity of the parties must remain confidential.

have been part of a plea deal was essentially nullified because the operator of the database failed to update their information.

This Article emerges from a rapidly developing area of law, data privacy and data sharing, focusing heavily on well-known concepts such as collateral consequences stemming from criminal recordkeeping, as well as due process and other constitutional protections.[16] Specifically, this Article examines how our society has developed several legal processes that have kept, and will continue to keep, civil death alive by attaching criminal[17] or negative civil stigma to individuals without adequate safeguards.[18] More specifically, I will discuss how these legal processes are now lowering the burden for government actors to attach negative stigma, criminal or civil, to individuals simply because we, as a society, are failing to recognize that our existing legal processes are quickly becoming antiquated given the rapid development of technology and our reliance upon technology to inform legally driven initiatives. If we, as a society, do not make an effort to consider the potential ramifications of permitting significant technological influence in the legal realm, we are opening a door that will expose individuals to unforeseen and potentially unintended punitive measures.

In essence, this Article highlights the importance of enacting adequate safeguards to ensure proper monitoring and control of any information stored in big data. This Article argues that inadequate safeguards in our existing legal processes may establish new, or exacerbate existing, collateral consequences such that citizens are no longer able to meaningfully participate or reintegrate into society following conviction, judgment, or a finding of responsibility. In a sense, we are witnessing how the modernization of the civil death as the impact of any collateral consequence is exacerbated by highly advanced and accessible technologies maintained by law enforcement or related recordkeeping entities. This Article focuses on three specific and representative examples of legal processes that

16. *See* U.S. Const. amend. V; *id.* amend. XIV, § 1 (guaranteeing that no person will be deprived of liberty or property without due process of law).

17. For purposes of this Article, "criminal stigma" refers to the "labeling and tagging processes . . . [that] identify[] an individual as criminal in the eyes of [the publics]" or otherwise suggest the potential for criminality or wrongdoing. *Mark of Cain – The Stigma Theory of Crime and Social Deviance*, U.S. Dep't Just. Off. Just. Programs, https://www.ojp.gov/ncjrs/virtual-library/abstracts/mark-cain-stigma-theory-crime-and-social-deviance [https://perma.cc/9BP8-JPVQ] (last visited Nov. 3, 2025).

18. Each of these processes is underappreciated by the public at large because the United States government, as well as its actors, have not facilitated open and transparent discussion of these legal processes.

are quietly depriving individuals of adequate procedural protections while attaching criminal or negative civil stigma. This Article further analyzes how these processes serve as information streams that flow into and contribute to much larger data reservoirs (i.e., big data), which further exacerbate potential collateral consequences and increases the exposure of individuals whose information is housed in said information stores.

First, I will address a process called "titling" in the United States military.[19] Titling, in its current form, is a process that has only been around since 2018. It involves procedures that permit military law enforcement to list an individual as the subject of an ongoing criminal investigation at a very early stage, often prior to adequate evidence being collected and without the benefit of a hearing or legal counsel.[20] After a service member is titled, that individual's identifying information is then placed into a federal law enforcement database, the Defense Central Index of Investigations ("DCII"), and is stored for up to 40 years, depending on the branch of service.[21] Even if charges are not formally filed or the person is ultimately absolved of any wrongdoing, the individual's information remains in the database simply because the service member was initially listed as the subject of an investigation (i.e., titled).[22] In order to expunge said

19. *See* ReAnne R. Wentz, *"Equality of Treatment": How Service Members of Color are Disproportionately Impacted by the Military Law Enforcement's Titling Process*, 230 Mil. L. Rev. 307, 311 (2023) ("Titling is a process unique to the military, in which the law enforcement agent will place the name of an individual in the subject block of a Law Enforcement Report (LER). Placing a name in the subject block occurs 'as soon as the investigation determines there is credible information that the subject committed a criminal offense.'").

20. *See Law Enforcement's Revenge in Military Justice*, L. Off. Jocelyn C. Stewart, https://www.ucmj-defender.com/law-enforcements-revenge-in-military-justice/ [https://perma.cc/XC8W-CADX] (last visited Sept. 8, 2025) ("Titling is not a judicial decision. In fact, being titled as the subject of an investigation does not mean you were charged with a crime at all . . . . [It] is not a decision to put a person into formal charging or the judicial (or even nonjudicial) process.").

21. Off. of Inspector Gen. of the U.S. Dep't of Def., DoD Instruction 5505.07: Titling And Indexing By DoD Law Enforcement Activities, 3 (Aug. 8, 2023), https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/550507p.pdf [https://perma.cc/3R3J-NL4N]; U.S. Dept. of Army, Privacy Act, *A0195-2b USACIDC* (Aug. 16, 2011), https://pclt.defense.gov/DIRECTORATES/Privacy-and-Civil-Liberties-Directorate/Privacy/SORNsIndex/Article/4012057/a0195-2b-usacidc/ [https://perma.cc/F5UD-7QV9].

22. *See* Wentz, *supra* note 19, at 311–13 (noting that titling information is retained in the DCII until the title individual takes action to have it expunged for lack of probable cause); *see also* L. Off. Jocelyn C. Stewart, *supra* note 20 ("The titling decision remains in a centralized database . . . ."); Off. of Inspector Gen. of the U.S. Dep't of Def., *supra* note 21, at 3 ("Once the subject of a criminal

information from the DCII, the service member, if the individual is even aware of this process,[23] must establish that (1) no probable cause or insufficient evidence existed to determine whether a crime occurred or (2) no probable cause or insufficient evidence existed to determine whether the person committed the crime, which, based on my independent research, is an almost insurmountable burden.[24] This is but one process through which law enforcement may attach negative stigma to an individual even if the person is ultimately found completely innocent or has their charges dropped. Undoubtedly, this process will expose individuals to unnecessary collateral consequences, potentially without any finding of wrongdoing, after their information is entered into big data (here, the DCII and potentially other databases). Depending upon who has access to a database housing the service member's information, the effect of any collateral consequence may vary greatly in scope and impact.

The next legal process I will address concerns an area of law that has been around for decades—Title IX—but has undergone rapid change recently and has become a seesaw political issue. I briefly begin by tracing the evolution of Title IX to show its significant expansion in scope, with the most drastic change occurring in 2011 following the Obama administration's issuance of the Dear Colleague Letter (hereinafter referred to as "the Letter"). This change reshaped the nature and scope of Title IX and redefined how sex-based discrimination is viewed and addressed on college campuses around the country.[25] Through the Letter, as well as subsequent amendments from the Trump and Biden administrations, post-secondary educational institutions now investigate and litigate Title IX misconduct matters through on-campus administrative

investigation is indexed in DCII, the information will remain in DCII, even if they are found not guilty, unless the DoD LEA head or designated expungement official grants expungement . . . .").

23. As discussed below, the military has no obligation to advise service members of the titling process or its potential effects.

24. *See* U.S. Dep't of the Army, Judge Advoc. Gen. Corps, "I've Been Titled!" What does that mean and how do I fix it?, https://home.army.mil/jackson/4417/4559/9054/Titling_and_Request_for_Amendment_to_DACID_Records.pdf [https://perma.cc/6PAV-VSJ3] (last visited Dec. 3, 2025).

25. *See* Russlynn Ali, U.S. Dep't of Educ., Dear Colleague Letter: Sexual Violence (Apr. 4, 2011), https://www.ed.gov/sites/ed/files/about/offices/list/ocr/letters/colleague-201104.pdf [https://perma.cc/XC6P-W8JW] ("This letter supplements the *2001 Guidance* by providing additional guidance and practical examples regarding the Title IX requirements as they relate to sexual violence . . . [and] by discussing the proactive efforts schools can take to prevent sexual harassment and violence . . . .").

disciplinary hearings.[26] Although my first article focused on this issue more broadly, this piece focuses on transcript notations placed on an individual's academic record either during the pendency of a disciplinary proceeding or following a finding of responsibility, which serves as a permanent, quasi-criminal record that follows the individual even if they transfer schools.[27] More specifically, this Article demonstrates that the placement of such a notation, such as a representation that the individual faced or is facing allegations involving sexual misconduct or other violent acts, such as robbery or battery, attaches significant criminal stigma without basic constitutional protections. In the criminal realm, a defendant will be afforded a host of due process and other constitutional protections prior to having such stigma permanently attached. As a matter of public safety, post-secondary institutions have a legal obligation to report any allegations involving crimes of violence, or related findings of responsibility, to the public and federal government.[28] As such, it is likely that this information is being stored in big data and may result in far-reaching, devastating collateral consequences for those responding to allegations or found responsible in Title IX proceedings, such as public perception, the ability to obtain certain employment, or even the opportunity to obtain a degree.

Finally, this Article directly addresses technology that law enforcement, including state, federal, and local agencies, utilize and rely upon when conducting daily business, such as assigning patrol routes, identifying high crime areas, investigating individuals, and even attaching stigma to those who are perceived to be at risk of conducting criminal activity (i.e., predicting crime, rather than reacting to it). For example, in 2012 the Los Angeles Police Department

26. *See* Naomi Mann, *Classrooms into Courtrooms*, 59 Hous. L. Rev. 363, 367–68 (2021) ("[The Department of Education's] 2020 Rule created a quasi-criminal courtroom system for Title IX investigatory proceedings, including disciplinary proceedings . . . .").

27. *See generally* Raymond Trent Cromartie, *Aequitas: Seeking Equilibrium in Title IX*, 49 U. Dayton L. Rev. 53, 53–58, 68 nn.70–80 (2023) (analyzing evolving Title IX procedures and the long-term impact of disciplinary records on accused students).

28. *See* U.S. Dep't of Educ., Clery Act Appendix for FSA Handbook 1 (2020), https://www.ed.gov/sites/ed/files/admins/lead/safety/cleryappendixfinal.pdf [https://perma.cc/2KML-U8HH] ("The Clery Act requires that all postsecondary institutions participating in title IV student financial assistance programs disclose campus crime statistics and other security information . . . [and] statistics, policies and programs related to dating violence, domestic violence, sexual assault, and stalking . . . ."); *The Jeanne Clery Act*, Clery Ctr., https://www.clerycenter.org/the-clery-act [https://perma.cc/P2X5-YDZX] (last visited Sept. 9, 2025) (discussing Clery Act requirements to disseminate annual public security reports with statistics of campus crime).

("LAPD") was one of the first agencies to begin utilizing a system designed by PredPol, a predictive policing company that allows law enforcement to store criminal data and run algorithms "to identify areas where future crime is most likely to occur."[29] Although law enforcement databases have long stored information regarding arrests or convictions, certain technology may, for example, harbor information about people who are simply stopped by police, among other things.[30] These systems not only rely upon preexisting data digitized from historical paper records, they also develop and learn as human actors add potentially biased information to the database or modify algorithms that facilitate the "proper" functioning of said technology.[31]

Since the technology relies on historical data and ongoing human input, I argue that it may be subject to developing prejudices or facilitating archaic racial norms depending upon the information that is fed into the system. It is well known that the LAPD has a strained history with its city and has been the subject of racial controversy, so it is not unreasonable to believe that the information digitized from that era may negatively affect how a supposed "unbiased" technology may predict crime or potential criminal actors.[32] For example, "black data," as one scholar observed, is data housed within database algorithms that attaches "permanent digital suspicion and targets poor communities of color."[33] This amplification

29. Sarah Brayne, *Big Data Surveillance: The Case of Policing*, 82 Am. Socio. Rev. 977, 989 (2017).

30. *Id.* at 992, 996 ("[T]he inter-institutional integration of data and proliferation of dragnet surveillance practices—including the use of data on individuals with no direct police contact and data gathered from institutions typically not associated with crime control—represent fundamental transformations with the very nature of surveillance.").

31. *See id.* at 1003–04 ("[B]ig data participates in and reflects existing social structures. Far from eliminating human discretion and bias, big data represents a new form of capital that is both a social product and a social resource . . . . Characterizing predictive models as 'just math,' and fetishizing computation as an objective process, obscures the social side of algorithmic decision-making. Individuals' interpretation of data occurs in preexisting institutional, legal, and social settings . . . .").

32. *See id.* at 998 ("These social dynamics inform the historical crime data that are fed into the predictive policing algorithm. However, once they are inputted as data, the predictions appear impartial; human judgment is hidden in the black box . . . under a patina of objectivity."); *see also* Ian Ayres & Jonathan Borowsky, A Study of Racially Disparate Outcomes in the Los Angeles Police Department (Oct. 2008), https://www.aclusocal.org/sites/default/files/wp-content/uploads/2015/09/11837125-LAPD-Racial-Profiling-Report-ACLU.pdf [https://perma.cc/844B-US3U].

33. Andrew Guthrie Ferguson, The Rise of Big Data Policing 3–4 (NYU Press 2017); *see also* Thomas P. Crocker, *Ubiquitous Privacy*, 66 Okla. L. Rev. 791, 791 (2014).

of existing racial animus, combined with the possibility of improper input from human actors, can attach criminal stigma to someone even if they have not committed a crime, thereby manifesting civil death by depriving that individual of due process prior to being so categorized. This potential impact is even more concerning given that law enforcement databases are often interconnected,[34] which further expands the scope of any disparate impact or collateral consequence. In essence, big data is functionally creeping.[35]

In exploring potential solutions to this issue, this Article ultimately proposes a two-prong approach. First, as briefly discussed above, we need to reexamine existing administrative and legal processes to ensure the current protections and procedural safeguards are adequate in light of big data's overwhelming influence in said proceedings, as well as the far-reaching impacts of any criminal record once it is housed in big data. Second, I assess safeguards already enforced by the General Data Protection Regulation ("GDPR"), data privacy legislation enacted by the European Union in 2016,[36] as well as legislation recently introduced in the United States, to emphasize the importance of robust oversight and auditing mechanisms for all law enforcement or other related databases.

This Article will advocate for additional safeguards that should be considered, and potentially implemented, in existing administrative and legal processes prior to placing any individual information in big data maintained and accessed by law enforcement or any related entities/individuals, as well as propose certain oversight and auditing procedures we should consider as technology continues to develop and influence our existing legal processes. For example, the Fourth Amendment of the United States Constitution generally protects individuals from unreasonable searches and seizures.[37] Prior to the introduction of technology, Fourth Amendment violations generally focused on physical searches of individuals or property.

---

34. *See generally* Jennifer Daskal, *Law Enforcement Access to Data Across Borders: The Evolving Security and Rights Issues*, 8 J. Nat'l Sec. L. & Pol'y 473, 501 (2016) ("Blocking provisions [against cross-border requests for data] in U.S. law are causing a backlash—resulting in countries seeking to unilaterally bypass these restrictions and/or demand that data be stored locally so as to avoid the U.S.-based legal restrictions on the sharing of sought-after data.").

35. *See* Bert-Jaap Koops, *The Concept of Function Creep*, 13 L., Innovation, & Tech. 29, 36 (2021) (defining functional creep as "the use of technology for new purposes beyond its originally intended purposes" and "the expansion of a . . . system or technology into areas for which it was not originally intended")

36. Council Regulation 2016/679, General Data Protection Regulation, 2016 O.J. (L 119) 53 (EU).

37. U.S. Const. amend. IV.

However, as technology has progressed, courts across the country began analyzing purported Fourth Amendment violations through a technological lens. In particular, two cases decided by the United States Supreme Court in the 1970s held that individuals are not entitled to an expectation of privacy when they voluntarily provide the relevant information to third-parties.[38] Since these ruling were issued, law enforcement and other government actors have heavily relied upon this principle to further countless investigations. Cases like *Smith* and *Miller* highlight the importance of courts and legal advocates recognizing the potential influence of technology upon individual rights.

Allowing the existing legal processes to proceed without adequate protections or other safeguards and then placing the aggrieved individual into big data will not only exacerbate collateral consequences, it will likely compromise public safety as an increasing number of people who have criminal or civil stigma attached to them struggle to find housing, employment, government benefits, and many other basic needs. The purpose of considering additional safeguards in existing legal processes is to curb the impact of big data until we have comprehensive, over-arching legislation that will address the long term. The longer we allow our antiquated legal processes to remain stagnant and fail to keep up with the rapid development of technology, the further we facilitate the modernization and re-introduction of civil death.

Where Part I of this Article provided a brief introduction to the concept of criminal recordkeeping and its transition to the digital realm, Part II will primarily focus on and explore the history of criminal recordkeeping and its impacts in the United States, as well as how advocates perceive the issue. Part III will then analyze and discuss the three processes that attach negative stigma to an individual without adequate safeguards, beginning with titling in the military, moving onto Title IX transcript notations, and concluding with law enforcement technologies. Finally, Parts IV and V will discuss existing data legislation, including the GDPR, provide brief background of legislation, analyze relevant provisions, and conclude by proposing safeguards that should be considered in the United States prior to storing an individual's information in big data. Through this Article,

38. *See* Smith v. Maryland, 442 U.S. 735, 744 (1979) ("[P]etitioner voluntarily conveyed numerical information to the phone company . . . . In so doing, petitioner assumed the risk that the company would reveal to police the numbers he dialed."); *see also* United States v. Miller, 425 U.S. 435, 443 (1976) ("This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party . . . .").

I will demonstrate that our society must strike a balance between promoting public safety and protecting individual rights and interests while implementing big data. By establishing adequate safeguards in existing legal processes and ensuring robust oversight of data-driven technology, we will hopefully mitigate adverse impacts or collateral consequences that may stem from the use of such technology.

## II.
## CRIMINAL RECORDKEEPING BACKGROUND AND IMPACTS

Prior to delving deeper into big data and the aforementioned legal processes that may contribute to said information stores, it is important to recognize the progression of criminal recordkeeping in the United States. The cataloging and indexing of information related to an individual's history of wrongdoing, whether criminal or civil, has an extensive past in our country. As mentioned above, our current legal system was heavily influenced by English common law and maintains its roots in the same.[39] Arguably, criminal recordkeeping began well before the founding of the United States through rather primitive forms of denoting wrongdoers from the general population, including branding with hot iron and local knowledge.[40] Although branding as a form of recordkeeping essentially disappeared by the eighteenth century, societies still sought a means to catalog and identify offenders.[41] Regardless of the progression of recordkeeping abroad, the American colonial system of criminal recordkeeping began to come into its own following the defeat of the British in the American Revolutionary War. Where the vast majority of colonial criminal or civil code was based largely in religion, with each colony maintaining its own legal system, constitution, and set of laws, post-colonial America, over time, began to develop a more robust system of criminal justice that centered on morality instead of religious tenets.[42]

---

39. *See* Chin, *supra* note 1, at 1790, 1793 (positing that the English common law punishment of civil death has reemerged in a new form within the United States criminal legal system).

40. *See* Terry Thomas, Criminal Records: A Database for the Criminal Justice System and Beyond 5–6 (2007) ("In the sixteenth century, branding had been a rudimentary means of letting the authorities know if they were dealing with a second-time offender.").

41. *See id.* (detailing early forms of criminal recordkeeping in the United States).

42. *See* Colonial Origins of the American Constitution: A Documentary History (Donald S. Lutz ed., 1998) (illustrating the role of religion in colonial American law); *see also* Jud Scott, *Civil Death in California: A Concept Overdue for Its Grave*, 15 Santa Clara L. Rev. 427, 430 (1975) (explaining that the Enlightenment

Following the founding of the United States in the late eighteenth century and the enactment of the United States Constitution, our legal system continued to expand and evolve, especially as the population and territory of the fledgling nation rapidly swelled. In fact, until the 1850s, criminal records primarily comprised of "rap sheets," originally referring to a simple note or other document prepared and maintained by local police, which notated basic information about an offender and substantively varied greatly among police departments.[43] Up until the 1960s, criminal records in the United States were kept in paper form, which generally required anyone seeking to obtain said information to physically present themselves at the court or agency where the documentation was housed to request it.[44] The eventual transition from paper to digital records was motivated by several factors including, but not limited to: (1) America's expansive territory, encompassing fifty states spanning almost four million square miles, which facilitated multi-jurisdictional offenders evading capture; (2) the development and availability of new technology; and (3) concerns related to efficient recordkeeping processes, especially when it came to information exchange among law enforcement and manually updating records.[45] The terms rap sheet and criminal record eventually became synonymous and expanded in scope thereafter, gradually encompassing more and more information, such as fingerprints and other biometrics, on individual offenders.[46]

In 1967, arguably the greatest expansion in criminal recordkeeping within the United States occurred. During that year, the Federal Bureau of Investigation's ("FBI") Criminal Justice Information Services Division was established.[47] In years past, the FBI maintained hard copies of criminal records, including fingerprints and other

---

Era shifted focus from severe punishment for transgressions to crime prevention and rehabilitation).

43. Off. of Tech. Assessment, An Assessment of Alternatives for a National Computerized Criminal History System 21–22 (1982).

44. *Id.* at 31–32.

45. *Id.* at 31–36.

46. *See Criminal Record*, Thesaurus.com, https://www.thesaurus.com/browse/criminal-record [https://perma.cc/8NGP-B7LG] (last visited Sept. 9, 2025); *see generally 100 Years of Fingerprints and Criminal History Records*, Fed. Bureau investigation (July 10, 2024), https://www.fbi.gov/news/stories/fbi-marks-100-years-of-fingerprints-and-criminal-history-records [https://perma.cc/L7NL-ZR6Y].

47. *See NCIC Turns 50: Centralized Database Continues to Prove Its Value in Fighting Crime*, Fed. Bureau Investigation (Jan. 27, 2017), https://www.fbi.gov/news/stories/ncic-turns-50 [https://perma.cc/75WG-BPQE] (noting that the Criminal Justice Information Services Division was formerly known as the Identification Division); *see also* U.S. Dep't of Just., Law Enforcement Records Management Systems,

biometric data. However, following a proposal to then-FBI Director J. Edgar Hoover, it began implementing a robust computer system that would act as a central repository for preexisting and future criminal records.[48] The primary purpose of this database was to create a centralized system that would house information from each state and disseminate the same to law enforcement agencies nationwide and abroad.[49] Following a collaborative effort among the FBI, United States Department of Commerce, and International Association of Chiefs of Police, an advisory board comprised of state and local police established specific policies and procedures for developing the criminal database.[50] After years of development, the National Crime Information Center ("NCIC") was formally launched on January 27, 1967.[51] Moving forward, the NCIC would house information related to felonies, misdemeanors, arrests, and criminal dispositions, among other things.[52]

While the progression to digital storage methods appeared to be initially positive on its face, public sentiment began to shift as the legitimacy of information stored in the NCIC, and similar databases developed later, came into question. For example, since its establishment, inaccurate or outdated information stored in the NCIC has resulted in false arrests or detainments, and even abuses in how the technology is implemented.[53] As referenced above, law enforcement in the United States has a long and complicated history of violence against the population, especially against underrepresented communities.[54] In fact, more than 1,300 people were

---

https://ucr.fbi.gov/law-enforcement-records-management-system [https://perma.cc/TP6H-AVEL] (last visited Dec. 2, 2025).

48. *See* Fed. Bureau Investigation, *supra* note 47.

49. *See* 28 C.F.R. §§ 20.1, 20.20–.21, 20.36 (2025) (referring repeatedly to the NCIC and similar databases as "central repositor[ies]").

50. *See* Fed. Bureau Investigation, *supra* note 47.

51. *Id.*

52. *See id*; *see also* Matthew Friedman, *Just Facts: As Many Americans Have Criminal Records as College Diplomas*, Brennan Ctr. for Just. (Nov. 17, 2015), https://www.brennancenter.org/our-work/analysis-opinion/just-facts-many-americans-have-criminal-records-college-diplomas [https://perma.cc/3CXC-HDZN].

53. *See* Alex Kane, *Terrorist Watchlist Errors Spread to Criminal Rap Sheets*, The Intercept (Mar. 15, 2016), https://theintercept.com/2016/03/15/terrorist-watchlist-errors-spread-to-criminal-rap-sheets/ [https://perma.cc/G48N-DGAA] (describing how the broad dissemination of highly inaccurate watchlists leads to false arrests and prejudicial treatment by courts and law enforcement, particularly for Muslim individuals).

54. *See Mapping Police Violence*, Campaign Zero, https://mappingpoliceviolence.org [https://perma.cc/C829-2SYP] (last visited Sep. 16, 2025) ("Black people are 2.8[ times] more likely to be killed by police than white people in the U.S.").

killed in 2024 as a result of police violence.[55] In the 1970s, our approach to crime and public safety was overhauled following a press conference by President Richard Nixon where he declared a war on drugs and crime.[56] Unfortunately, the adverse impacts of President Nixon's now infamous speech are still being felt today through the lingering effects of mass incarceration.[57] As a study conducted by the Department of Justice found, the number of Americans who have a college degree is similar to the number of Americans who have a criminal record.[58] While crime rates have generally decreased since the 1990s, this trend reversed for some violent crimes starting in 2020, and it may still take decades to balance the damage caused by President Nixon's policies.[59] America's sudden shift toward aggressive prosecution of crime and the imposition of drastic sentences resulted in mass incarceration and conviction, which served as a catalyst for collateral consequences as more and more citizens were being exposed to legal proceedings and the associated stigma.[60]

---

55. *Id.* This data includes incidents classified as suicide by police and involving off-duty officers. *See Mapping Police Violence: Data and Methodology*, Campaign Zero (Sept. 20, 2025), https://mappingpoliceviolence.org/methodology [https://perma.cc/D478-JEMZ].

56. *See* Brian Mann, *After 50 Years of the War on Drugs, 'What Good Is It Doing for Us?*,' NPR (June 17, 2021), https://www.npr.org/2021/06/17/1006495476/after-50-years-of-the-war-on-drugs-what-good-is-it-doing-for-us [https://perma.cc/4EDV-3YZT] (referencing President Nixon's June 17, 1971 speech as the symbolic start of the modern drug war).

57. *See* James Cullen, *The History of Mass Incarceration*, Brennan Ctr. for Just. (July 20, 2018), https://www.brennancenter.org/our-work/analysis-opinion/history-mass-incarceration [https://perma.cc/6FT5-EQCG] ("The U.S. incarcerates more people than any nation in the world, including China. And the U.S. is also the leader in the prison population rate . . . . Nixon started this trend, declaring a 'war on drugs' and justifying it with speeches about being 'tough on crime.'"); *see also* Rebecca Vallas & Sharon Dietrich, *One Strike and You're Out: How We Can Eliminate Barriers to Economic Security and Mobility for People with Criminal Records*, Ctr. for Am. Progress (Dec. 2, 2014), https://www.americanprogress.org/article/one-strike-and-youre-out/ [https://perma.cc/A55U-9ADG] ("[R]esearch shows that mass incarceration and its effects have been significant drivers of racial inequality in the United States, particularly during the past three to four decades.").

58. *See* Friedman, *supra* note 52.

59. *See* John Gramlich, *What the Data Says About Crime in the U.S.*, Pew Rsch. Ctr. (Apr. 24, 2024), https://www.pewresearch.org/short-reads/2024/04/24/what-the-data-says-about-crime-in-the-us/ [https://perma.cc/326J-3JXA] (noting that the rates of violent crime and property crime fell 50–70%, depending on the data source, from 1993 to 2022, but the murder rate increased sharply during the COVID-19 pandemic).

60. *See id.* Although the two primary sources of criminal data are the FBI and the Bureau of Justice Statistics ('BJS'), the data is not entirely complete as these entities rely upon information reported to them by other law enforcement entities spread

This amassing of criminal records laid the foundation for our now technically-driven processes as that documentation and information is still being housed in databases and relied upon by those who have access to said information.[61]

Currently, criminal records are housed at several levels within the United States and originate from an untold number of sources. In fact, since the establishment of the NCIC, each state has developed and maintained its own criminal recordkeeping databases.[62] For example, at the federal level, in addition to the NCIC, the United States government has established and maintains: (1) the Interstate Identification Index ("III"), a digital index of information acquired by law enforcement from a suspect and housed within the NCIC[63]; (2) the National Instant Criminal Background Check System ("NICS"), which is primarily used for FBI screening of potential purchasers of firearms[64]; (3) the Integrated Automated Fingerprint Identification System ("IAFIS"), a national database that stores biometric data and other criminal history[65]; (4) the National Driver Register and Problem Driver Point System, a system that stores information related to motor vehicle offenses including, but not limited to, suspended and revoked licenses, convictions related to driving under the influence of substances, falsifying records, and motor vehicle accidents resulting in injury or death[66];

---

throughout the country. According to data, the FBI and BJS only obtained statistics from 83% of participating law enforcement entities in 2022.

61. *See* Friedman, *supra* note 52.

62. *See State Identification Bureau Listing*, Fed. Bureau Investigation, https://www.fbi.gov/how-we-can-help-you/more-fbi-services-and-information/identity-history-summary-checks/state-identification-bureau-listing [https://perma.cc/3KGH-JJDF] (last visited Oct. 7, 2025) (listing the state identification bureaus in the fifty U.S. states plus Washington D.C., Puerto Rico, Guam, and the U.S. Virgin Islands).

63. *See* 28 C.F.R. § 20.36 (describing participation in the III System).

64. *See About NICS*, Fed. Bureau Investigation, https://www.fbi.gov/how-we-can-help-you/more-fbi-services-and-information/nics/about-nics [https://perma.cc/HV2F-8MMC] (last visited Sep. 18, 2025) (the III system, "was established as a result of the Brady Handgun Violence Prevention Act of 1993 [ ]" which requires federally licensed firearm dealers to perform a search in the national background check system to determine if a person can legally buy or own a gun).

65. Crim. Just. Info. Servs. Div., *The Integrated Automated Fingerprint Identification System,* Fed. Bureau Investigation, https://ucr.fbi.gov/fingerprints_biometrics/biometric-center-of-excellence/files/iafis_0808_one-pager825 [https://perma.cc/X2GT-6346] (last visited Oct. 7, 2025).

66. *See The National Driver Register (NDR) and Problem Driver Pointer System (PDPS)*, Nat'l Highway Traffic Safety Admin., https://www.nhtsa.gov/research-data/national-driver-register-ndr [https://perma.cc/2TNF-LDF9] (last visited Sept. 2, 2025) ("[T]he Problem Driver Point System . . . contains information on individuals whose privilege to operate a motor vehicle has been revoked, suspended, canceled or denied

(5) Secure Flight, a "risk-based passenger prescreening program that enhances security by identifying low and high-risk passengers before they arrive at [an] airport by matching their names against trusted traveler lists and watchlists"[67]; and (6) importantly, Nlets, or the International Justice & Public Safety Network and formerly the National Law Enforcement Telecommunications Systems, which is an interface that allows users to access databases maintained by each state, essentially forming a nationwide network of interconnected law enforcement databases.[68] As mentioned above, the development and use of the aforementioned systems, among others, has been the subject of heated debate. Where one side hails law enforcement databases and technologies as a pillar of public safety and efficiency, others question the rapid expansion and ethical implementation of such processes, as well as the undoubted exacerbation of existing collateral consequences.[69]

The arguments from advocates of a robust criminal recordkeeping system are straightforward. They assert that such recordkeeping processes permit the efficient storage and exchange of information among law enforcement while promoting public safety, thus serving as an invaluable tool for law enforcement.[70] As advocate scholars have noted, "[p]ublic safety benefits significantly outweigh any burden that some collateral consequences place on an ex-offender's ability to reintegrate into society."[71] The argument surrounding

---

or who have been convicted of serious traffic-related offenses."); *see also* Nat'l Highway Traffic Safety Admin., The National Driver Register (2006), https://www.nhtsa.gov/sites/nhtsa.gov/files/ndr.pdf [https://perma.cc/5GXZ-RL53].

67. *DHS Announces Extension of REAL ID Full Enforcement Deadline*, Dep't Homeland Sec. (Dec. 5, 2022), https://www.dhs.gov/archive/news/2022/12/05/dhs-announces-extension-real-id-full-enforcement-deadline [https://perma.cc/D7P8-TDGJ].

68. *What We Do*, Nlets, https://nlets.org/about/what-we-do [https://perma.cc/W8N8-4BHZ] (last visited Sept. 2, 2025).

69. *See* J.J. Prescott & Sonja B. Starr, *Expungement of Criminal Convictions: An Empirical Study*, 133 Harv. L. Rev. 2460, 2552 n.345 (2020) (contrasting a scholarly work claiming public safety is best served by access to criminal history data with another arguing that safety is increased when those with past convictions can productively participate in society).

70. *See* Wentz, *supra* note 19, at 325 ("[L]aw enforcement agencies . . . believe that . . . indexing . . . merely 'create[s] an administrative index of investigations, searchable by subject name or other identifying data' and maintain that [it] is a vital tool for investigators." (fourth alteration in original)).

71. John G. Malcolm & John-Michael Seibler, *Collateral Consequences: Protecting Public Safety or Encouraging Recidivism?*, Heritage Found. 2 (2017), https://www.heritage.org/crime-and-justice/report/collateral-consequences-protecting-public-safety-or-encouraging-recidivism [https://perma.cc/D9KN-HHNB]; *see also* Roberts, *supra* note 4, at 334 (discussing "commonly-held" view that "giving the public full access to information about individuals' criminal history advances public safety.")

public safety also focuses on insulating employers from individuals with a criminal record. In fact, a survey performed by the Society of Human Resource Management found that 52% of employers who performed background checks primarily check an applicant's background to limit potential legal liability, while only 49% and 17% performed a check to foster a safer work environment and assess the character of an applicant, respectively.[72] The process of exploring an individual's background for employment purposes is well understood. For example, failing to exercise due diligence in the hiring, supervision, and retention of an employee or representative may result in significant monetary and legal exposure for an employer if injury occurs to another person or property as a direct and proximate result of the worker's acts or omissions made in furtherance of their employment.[73] This is a prime example of one of the many ways big data can further public safety without unnecessarily sacrificing individual rights and opportunities.

Opponents of extensive criminal recordkeeping counter the overarching public safety concern by arguing that collateral consequences[74] actually present a greater threat to public safety than one

72. *See* Friedman, *supra* note 52. For example, if a delivery company hires a truck driver who has a history of driving under the influence and that employee subsequently injures or kills someone while driving intoxicated on the job, the employer could face civil claims that may vicariously impute the employee's negligence upon the employer. Another example may be any occupation where an individual is placed in a position of responsibility over others, such as an elementary school teacher. Undoubtedly, it is within the employer's and the public's best interest to ensure that individual does not have a history of child abuse or other issues that may endanger the children. *See generally Respondeat Superior*, Black's Law Dictionary (12th ed. 2024) ("The doctrine holding an employer or principal liable for the employee's or agent's wrongful acts committed within the scope of the employment or agency.").

73. *See* Stuart M. Speiser, Charles F. Krause & Alfred W. Gans, American Law Of Torts § 4:3 (Monica C. M. Leahy ed., 2025) ("The doctrine of respondeat superior imputes vicarious liability from an employee to an employer when the employee's acts are within the scope of the authority conferred.").

74. Collateral consequences may impact employment, transportation, licensure, education, immigration status, child custody, voting rights, one's ability to purchase a firearm, housing, entitlement to benefits, reputation, and even legal standing. *See, e.g.*, Legis. Analysis and Pub. Pol'y Assoc., Collateral Consequences of Criminal Justice Involvement 1 (2024), https://legislativeanalysis.org/wp-content/uploads/2024/10/Collateral-Consequences.pdf [https://perma.cc/V72M-8ZQD] ("[Collateral] consequences include but are not limited to: (1) the loss of the rights to vote, serve on a jury, or possess a firearm; (2) barriers in obtaining housing, employment, higher education, professional licensure, and federal and state government benefits; and (3) barriers in obtaining credit and loans, including student loans."); Fed. R. Evid. 608 and 609 (permitting the introduction of a prior criminal conviction for purposes of impeachment and attacking a witness's credibility, subject to certain exceptions); U.S. Dep't of Just., Criminal Resource Manual: 8 U.S.C.

might imagine.[75] Many states, recognizing that collateral sources increase the likelihood that an ex-offender may commit another crime due to instability, currently maintain "clean slate" and/or "ban the box" legislation that recognizes collateral consequences and seeks to mitigate their impact.[76] The opposition's focus upon collateral consequences is not only a result of conditions surrounding post-conviction or post-judgment life, but also stems from potential inaccuracies that may exist in law enforcement databases.[77] Depending upon nature and substance, the existence of any inaccurate information within a criminal record or database may unnecessarily expose an individual to collateral consequences. This concern is heightened by the fact that we exist in a digital age where information introduced into a technological realm, like the Internet or a database,

---

1326, https://www.justice.gov/archives/jm/criminal-resource-manual-1912-8-usc-1326-reentry-after-deportation-removal [https://perma.cc/25SF-A692] (last visited Dec. 2, 2025); Bobby Dale Barina, *How Can a Criminal Conviction Affect Child Custody?*, Barina Law Group (Dec. 27, 2022), https://www.bobbybarinalaw.com/how-can-a-criminal-conviction-affect-child-custody/ [https://perma.cc/BB94-WBQX].

75. *See* Christi M. Smith, *The Pathway to Prosperity: How Clean Slate Legislation Enhances Public Safety and Stimulates the Economy*, R Street, at 2, 8 (Mar. 14, 2023), https://www.rstreet.org/research/the-pathway-to-prosperity-how-clean-slate-legislation-enhances-public-safety-and-stimulates-the-economy/ [https://perma.cc/HK9S-4RRJ] ("Record-based discrimination is extremely costly to taxpayers and the overall economy, resulting in an estimated $78–$87 billion loss in the national gross domestic product . . . . Collateral consequences . . . are extremely costly to all Americans, jeopardizing public safety and the national economy. The rate of recidivism for people on community supervision and the increased likelihood of rearrest among this population is largely attributed to the criminogenic nature of prison and the lack of access to a social safety net upon release.").

76. *See id.* at 15 (defining clean slate legislation as "a policy model that uses technology to automate arrest- and conviction-record clearance if a person stays crime-free for a specified period of time."); Beth Avery and Han Lu, *Ban the Box: U.S. Cities, Counties, and States Adopt Fair Hiring Policies to Advance Employment Opportunities for People with Past Convictions,* Nat'l Emp. L. Project, at 2 (Oct. 1, 2021), https://www.nelp.org/insights-research/ban-the-box-fair-chance-hiring-state-and-local guide/ [https://perma.cc/7H5T-R8LW] (identifying ban the box legislation as "policies [that] provide applicants a fair chance at employment by removing conviction and arrest history questions from job applications and delaying background checks until later in the hiring process.")

77. *See* Sarah Lageson, *Criminally Bad Data: Inaccurate Criminal Records, Data Brokers, and Algorithmic Injustice*, 2023 U. Ill. L. Rev. 1771, 1773–74 ("One analysis of 200 New York state rap sheets identified an 80% error rate. A federal analysis found that a criminal-background-checking system used for governmental workers incorrectly reported criminal history records for employees 42% of the time . . . . Inaccurate reports constitute the bulk of complaints filed with the Bureau of Consumer Financial Protection; 191,000 such complaints were filed in 2020 alone.").

may never disappear, especially considering private companies are exploiting information for profit. As one scholar noted:

> Criminal justice agencies maintain and work to update their own online databases, but th[is] publicly available data [has] often already leaked onto unregulated, unofficial websites. A routine, informal Internet search might reveal a criminal history posted on a neighborhood crime watch blog or a background check company might reveal part of a criminal record . . . .[78]

Understandably, the fear is that individual rights are being eroded by technology while it enhances the ability of government actors to pursue legal claims against individuals. Essentially, the cards are being stacked against individual citizens.

Historically, much like our criminal justice system and law enforcement generally, collateral consequences disparately affect minorities and other underrepresented communities. In fact, a 2009 study found that Black men who have a criminal record were twice as likely as their White counterparts to be viewed negatively by potential employers.[79] Additionally, Blacks and Latinos are more likely to have inaccuracies in their criminal records.[80] These findings are more troubling given that Blacks generally report that they are treated less fairly than Whites when interacting with law enforcement[81] and

78. Sarah Esther Lageson, *Digital Punishment's Tangled Web*, 15 CONTEXTS 22, 24 (2016) https://contexts.org/articles/digital-punishments-tangled-web/ [https://perma.cc/VAS8-VD8W].

79. *See* Roberts, *supra* note 4, at 331 ("[B]lack men with a record who applied [to an entry-level job] were twice as likely as white men to be saddled with this 'criminal record penalty.'") (citing Devah Pager, Bruce Western & Naomi Sugie, *Sequencing Disadvantage: Barriers to Employment Facing Young Black and White Men with Criminal Records*, 623 ANNALS AM. ACAD. POL. SOC. SCI. 195, 199 (2009)).

80. *See* MARTIN WELLS ET AL., CRIMINAL RECORD INACCURACIES AND THE IMPACT OF RECORD EDUCATION INTERVENTION ON EMPLOYMENT-RELATED OUTCOMES 16–17 (2020), https://ecommons.cornell.edu/server/api/core/bitstreams/06046ce4-114f-4252-b3a1-8bec84529540/content [https://perma.cc/8RNW-UFRX] ("To summarize, we find that respondents who identified as African American or Black are disproportionately likely to have inaccuracies on their criminal records. They have higher rates of inaccuracies than Latinos and whites, while Latinos have higher rates of inaccuracies than Whites.").

81. *See* John Gramlich, *From Police to Parole, Black and White Americans Differ Widely in Their Views of Criminal Justice System*, PEW RSCH. CTR. (May 21, 2019), https://www.pewresearch.org/short-reads/2019/05/21/from-police-to-parole-black-and-white-americans-differ-widely-in-their-views-of-criminal-justice-system/ [https://perma.cc/4RKD-E4EN] ("84% of [B]lack adults said that, in dealing with police, [Black people] are generally treated less fairly than whites. . . . 63% [of White people] said the same.").

navigating the criminal justice system in general.[82] Accordingly, the dynamics between races and law enforcement in the United States is a central issue when analyzing the utility of criminal databases and similar recordkeeping processes as a facilitator of public safety.

Prior to proceeding, I will provide a brief real-life example of how inaccurate information housed in big data may impact an individual in unforeseen ways simply because it exists on the Internet or in a database. I currently assist with teaching the civil litigation clinic at the University of Denver as a graduate fellow. In our clinic, our student attorneys represent indigent or underrepresented individuals in a variety of civil matters, and the students do so under Colorado's Student Practice Act, a law that permits them to practice under a barred attorney's license as if they are lead counsel. Although I did not supervise the matter personally, our clinic recently represented an individual seeking a civil protection order against her ex-partner in county court and sought to make the order permanent. As the students prepared for trial, they discovered a privately maintained online database that contained outdated information related to the respondent and had potential relevance in the current dispute. Notably, the students noticed that the online database contained information related to a now expunged criminal record associated with the respondent. After heated argument at trial, the court ultimately permitted introduction of the evidence, which eventually contributed to a permanent civil protection order being entered against the respondent. While we were able to obtain justice for our client, the respondent was not aware of the online database and thought that his expungement would have been effective at the time he entered a plea or completed his sentence. However, due to a privately owned database that contained inaccurate information, the respondent again faced detrimental impact from a legal proceeding that he thought was concluded. The risk of big data in this example is clear. The legitimacy of certain legal and administrative processes is at risk since they may eventually be usurped by unregulated and inaccurate information contained in big data.

## III.
## DISCUSSION

As mentioned above, this Part will focus on three unique, arguably deficient, legal processes that exist in the United States and

82. *See id.* ("[A]round nine-in-ten [B]lack adults (87%) said blacks are generally treated less fairly by the criminal justice system than whites, a view shared by a much smaller majority of white adults (61%).").

attach criminal stigma to an individual without adequate constitutional protections or other safeguards. The first is titling in the United States military, a process that is exclusive to service members but generally extends far beyond their time in the military.[83] The next process that will be addressed is the use of transcript notations during Title IX disciplinary proceedings on college campuses, regardless of the allegations a respondent is facing.[84] Finally, this Part will analyze criminal recordkeeping databases and technologies maintained by law enforcement or similar entities, and how those systems are now rapidly expanding and developing in unforeseen and unintended ways (i.e., functionally creeping). Specifically, I will discuss technology evolving from a process once focused on documenting and indexing information on criminal offenders that has since progressed to one largely focused on predicting crime. In fact, current technology now houses information related to not only individuals who are criminal offenders, but also people who have committed no crime, thereby potentially attaching negative stigma without any due process or other notice.[85]

### *A. Titling in the United States Military*

As a preliminary matter, it is important to recognize that the United States military is governed by the Uniform Code of Military Justice ("UCMJ"), a federal law enacted in 1951 that applies to every single member of the United States Military and excludes private citizens.[86] Since the UCMJ is separate and distinct from the civilian criminal justice system, this Article only addresses relevant differences between the civilian and military justice systems and will only focus on the titling process, which is not implemented in the civilian realm. Still, the titling process is a prime example of how our society allows individual rights to be eroded in the name of public safety.

83. The discussion about titling in the military will not be limited to a certain branch and will only address major differences in any branch-specific titling process.

84. This Article will only focus on Title IX proceedings at the post-secondary level and will not delve into other areas where Title IX is litigated, such as lower levels of education (i.e., high school, elementary school, etc.)

85. *See* Nicol Turner Lee & Caitlin Chin-Rothmann, *Police Surveillance and Facial Recognition: Why Data Privacy Is Imperative for Communities of Color,* Brookings Inst. (Apr. 12, 2022), https://www.brookings.edu/articles/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color/ [https://perma.cc/ETP7-FMYJ] ("[L]aw enforcement agencies often rely upon tools developed within the private sector, and, in certain cases, can access massive amounts of data either stored on private cloud servers or hardware . . . or available in public places like social media or online forums.").

86. *See* 10 U.S.C. § 802 (encompassing active-duty personnel, reservists, members of the National Guard, some civilians in support roles, and cadets).

The UCMJ has developed over the years and began implementing titling prior to 1992, when significant changes were enacted.[87]

> Under the pre-1992 titling standard, the [Criminal Investigation Division (CID)] temporarily indexed information [about servicemembers] in the DCII . . . upon completion of the initial [investigative report]. The CID did not complete permanent indexing until . . . probable cause existed to believe that an offense was committed and that the "suspect" committed that offense.[88]

The current standard for titling is much lower. Formally defined:

> Titling is a process . . . in which the law enforcement agent will place the name of an individual in the subject block of a Law Enforcement Report ("LER")[89] . . . 'as soon as the investigation determines there is credible information that the subject committed a criminal offense.'[90]

Credible information "can be as little as an alleged victim's first statement to military police [and] doesn't mean he or she actually committed any crime."[91] Should probable cause be established later in the military investigation, the DCII entry will be updated to "founded," and the entry forwarded to the FBI's NCIC.[92] As one scholar noted, a "founded" designation sometimes occurs well before an investigator legally establishes probable cause, a standard that must be met in both civilian and military criminal investigations

87. *See* Patricia A. Ham, *The CID Titling Process—Founded or Unfounded?*, Army Law., Aug. 1998, at 1, 6–8 (detailing the titling standards pre-1992 and explaining the 1992 changes to the standard).

88. *Id.* at 6.

89. Formerly known as "Reports of Investigation" and defined as "[a]n official record of all pertinent information and facts obtained in a . . . law enforcement report or criminal investigation." Wentz, *supra* note 19, at 311 n.17; U.S. Dep't of the Army, Army Regulation 195-2: Criminal Investigation Activities 45 (2020).

90. Wentz, *supra* note 19, at 311; s*ee also* Off. of Inspector Gen. of the U.S. Dep't of Def., *supra* note 21, at 7 (defining "credible information" as "[i]nformation disclosed or obtained by a [criminal investigator] that, considering the source and nature of the information and the totality of the circumstances, is sufficiently believable to lead a trained [investigator] to *presume the facts or facts in question are true*." (emphasis added)).

91. *Titling Removal Actions*, Mil. Just. Att'ys, https://www.militaryjusticeattorneys.com/practice-areas/administrative-appeals-rebuttals/titling-actions/ [https://perma.cc/SB2E-L5C8] (last visited Sept. 9, 2025).

92. *See* U.S. Dep't of the Army, Army Regulation 190-45: Military Police: Law Enforcement Reporting 28–30 (2016) (describing "founded offenses" as those supported by probable cause that a servicemember was the "subject" of the offense and mandating the reporting of such offenses in the DCII and to the NCIC).

prior to arresting an individual or searching their property.[93] Although a definition of probable cause is not explicitly provided within the United States Constitution, the Fourth[94] and Fourteenth[95] Amendments have been interpreted by courts to generally require facts and circumstances that, "at the moment the arrest [or search] was made, . . . [were] within [the] knowledge [of law enforcement]" based upon "reasonably trustworthy information . . . sufficient to warrant a prudent [person] in believing that the [suspect] had committed or was committing an offense."[96] In essence, titling is purely an investigative decision, not a legal one, especially since there is very little involvement by any counsel at this stage of the investigation.[97] As discussed in greater detail below, this lower standard (i.e., designating allegations as "founded") does nothing but significantly increase the exposure for current and former service members, especially given the fact that an untold number of individuals and entities have access to the information stored in the DCII and NCIC.[98]

Once a military investigator determines there is credible information, a service member is formally titled and his or her information[99] is then entered into the DCII, as well as other law enforcement databases, for up to 40 years.[100] Unfortunately, once a service member is entered into the DCII, the individual's fate is largely sealed as the burden of removing oneself from these databases is

93. *See* Wentz, *supra* note 19, at 311–12 (noting that titling and indexing uses a standard lower than probable cause).

94. U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularity describing the place to be searched, and the persons or things to be seized.").

95. U.S. CONST. amend. XIV (providing the same due process protections against state governments and generally granting citizens "equal protection of the laws.").

96. *See* Beck v. Ohio, 379 U.S. 89, 91 (1964).

97. *See* Wentz, *supra* note 19, at 311 (noting that an individual is titled as soon as there is credible information that they have committed an offense).

98. *See* Ham, *supra* note 87, at 4–5 ("As of 1994 . . . the DCII contained over twenty-nine million indices on approximately nineteen million individuals, and it was growing at a rate of about two million indices per year. . . . Access to information in the DCII is widespread. The DCII receives an average of 35,000 requests per day. Twenty-seven agencies are authorized access and input to the DCII, with a total of 1179 terminals.").

99. Information may include not only the person's biographical data (name, date of birth, social security number, etc.), but also DNA and any information contained within the investigative report at the time of titling. *See* U.S. DEPT. OF ARMY, *supra* note 21, at 8.

100. *See* Wentz, *supra* note 19; *see also* U.S. DEPT. OF ARMY, *supra* note 21.

nigh insurmountable, assuming the service member is even aware he or she is titled.[101] In fact, the United States military is not required to provide an affirmative advisement on titling, so service members and veterans who are entered in the system may not recognize this process until an adverse impact is triggered by an inquiry.[102] Again, service members can be titled even if charges are never formally brought or the person is found completely innocent.[103] Yet, Department of Defense policy clearly indicates that titling is not intended to "imply

101. *See* Rachel Fobar, *They've Never Been Arrested. Why Does the FBI List Thousands of Service Members as Potential Criminals?*, War Horse (Oct. 23, 2025), https://thewarhorse.org/service-member-flagged-military-titling/ [https://perma.cc/S8RW-R9AS] ("'They've created a system where you're guilty until proven innocent,' [said a former Army colonel who specializes in defending service members]. 'If the [Army Criminal Investigation Division] agent believes something, then you're going to have this criminal history created, and it's up to you to now prove that it didn't happen.' (second alteration in original)); *see also* Matt Hill, *Titling in the Military [In]Justice System*, SOFREP (Mar. 26, 2021), https://sofrep.com/news/titling-in-the-military-injustice-system/ [https://perma.cc/5V9K-HZ4E] ("Many in the public arena aren't aware of titling and have no knowledge of its current meaning or use . . . . [I]n the four years I served in the Marine Corps I never heard the word used even once.").

102. Although I will not fully recite the facts and circumstances surrounding a sexual assault investigation where I was named the defendant during my time in the Army, my initial article provides a more thorough overview. Cromartie, *supra* note 27, at 58–60. In summary, while I was found not guilty of all sexual charges, I was found guilty of providing a false official statement during my initial interrogation. *Id.* As a result of the investigation, I was titled and entered into the DCII and likely other law enforcement databases; however, I was never advised of this fact and did not become aware of it until years later. In February 2023, I visited Buckley Air Force Base, located in Aurora, Colorado, to shop with my significant other. As is standard procedure, we initially presented at the base visitor center to obtain a guest pass by providing my driver's license to the guard. After approximately 10–15 minutes, the gate guard returned and informed me that I was denied entry to the base. I quickly inquired as to the reasoning and was then informed that I had an open sexual assault investigation from 2013 (i.e., my criminal investigation from West Point, which was fully resolved in June 2013, was never administratively closed by the military). Although I pleaded my case and informed the guard of this substantial error, I was instructed to contact the United States Air Force and Army. Following months of administrative appeals, with the assistance of Senator John Hickenlooper's office, my entry in the DCII was updated on July 25, 2023. Based on correspondence from the United States military, my information was corrected to accurately reflect the disposition of my case ten years after the fact. Letter from Michelle Kardelis, Chief, FOIA/PA Div., to Raymond Trent Cromartie (July 25, 2023) (on file with author). It is unclear how this inaccuracy may have negatively affected my life prior to my discovery as the titling process was not recognized by me until I faced a negative consequence.

103. *See generally* Off. of Inspector Gen. of the U.S. Dep't of Def., *supra* note 21, at 3 ("Titling and indexing are administrative procedures and will not imply any degree of guilt or innocence . . . . Once the subject of a criminal investigation is

any degree of guilt or innocence," which appears contrary to the practical impact.[104]

Any impact of titling is exacerbated by the fact that limited avenues for relief exist, which is largely due to the significant burden placed upon an individual seeking respite. Under the current version of the regulation, government expungement officials can only remove a titled individual's information if:

> (1) Probable cause did not or does not exist to believe that the offense for which the covered person was titled and indexed occurred, or insufficient evidence existed or exists to determine whether such offense occurred[;]
>
> (2) Probable cause did not or does not exist to believe that the covered person committed the offense for which they were titled and indexed, or insufficient evidence existed or exists to determine whether they committed such offense[; or]
>
> (3) Such other circumstances as the DoD LEA head or expungement official determines would be in the interest of justice . . . .[105]

The regulation further permits decision-makers to rely upon

> [t]he extent or lack of corroborating evidence against the covered person with respect to the offense[;] . . . [w]hether adverse administrative, judicial, or other such action was initiated against the covered person for the offense[;] . . . [and] [t]he type, nature, and outcome of any adverse administrative, disciplinary, judicial, or other such action taken against the covered person for the offense.[106]

Based on a comprehensive review of appellate case decisions, appellants are rarely granted the relief they seek.[107] This is not surprising given the appellant must essentially argue against the methodology and reliability of any investigator's findings and rebut a finding of probable cause.

Much like the other two processes discussed below, titling results in significant collateral consequences and negative stigma

---

indexed in DCII, the information shall remain in DCII, even if they are found not guilty . . . .").

104. *See id.*

105. *Id.* at 5.

106. *Id.*

107. *See generally* U.S. Dep't of Def., Boards of Review Reading Rooms, https://boards.law.af.mil/ [https://perma.cc/7M5L-HFZS] (last visited Sep. 8, 2025).

without due process or other adequate safeguards. Again, the impact of collateral consequences is primarily felt due to the indefinite scope of information dissemination via big data.[108] While an active service member may face unique consequences due to being titled during their military career, such as being "flagged"[109] or passed up for promotion, both current and former service members may experience the full extent of collateral consequences in their civilian capacity. For example, a veteran's ability to purchase a firearm or obtain professional licensure might be affected depending upon the information stored in the DCII, NCIC, or other database.[110] Further compounding the potential impact of any collateral consequence is the fact that a study has shown DCII users "misunderstand the purpose of the [database] and [the] uses of the criminal investigative data contained therein, and that additional training of . . . DCII users is necessary."[111] Meaning, service members may be erroneously titled and entered into the databases simply because the responsible personnel have not received adequate training and fail to appreciate the significance of a titling decision.

If the standard for entering a service member into the DCII is based largely on the perception of a trained investigator and the sufficiency of training has already been called into question by a

108. The DCII, much like many other law enforcement databases, is interconnected with other information stores, creating a network of big data.

109. *See What It Means to be "Flagged" – For Military Justice*, L. Off. Jocelyn C. Stewart, https://www.ucmj-defender.com/what-it-means-to-be-flagged-for-military-justice/ [https://perma.cc/7S67-A2HK] (last visited Sept. 3, 2025) ("When a Soldier is flagged by the Army, it means that he [or she] is not eligible for certain favorable personnel actions. These actions include reenlistment, a permanent change of station . . . military awards and decorations, and military schools. It can also interfere with non-military activities that are based on service, such as using tuition assistance benefits . . . . A flag can be initiated by the commander for a variety of reasons, such as . . . being arrested or convicted of a crime, or being under investigation for misconduct."). For example, during my criminal investigation, I was not permitted to leave the base overnight or attend events, among other things.

110. *See The Impact of a Military Record: Long-Term Consequences and Mitigation*, Griffin L. Firm (Oct. 6, 2024), https://www.griffinlawdefense.com/blog/2024/october/the-impact-of-a-military-criminal-record-long-te/ [https://perma.cc/H6DZ-MFYF] ("A military criminal record can affect fundamental rights such as voting and firearm possession, complicate immigration status for non-citizens, and impact security clearances vital for certain jobs."); Margaret Love, *NH Limits Denial of Licenses Based on Criminal Record*, Collateral Consequences Res. Ctr. (July 10, 2018), https://ccresourcecenter.org/2018/07/10/16794/ [https://perma.cc/47FQ-4KCM].

111. U.S. Dep't of Def., Department of Defense Policy Concerning Titling and Indexing of Individuals in the Defense Clearance and Investigations Index 6 (2002), https://apps.dtic.mil/sti/pdfs/ADA400229.pdf [https://perma.cc/X8YK-MUHM].

government-funded study, then certainly we need to review titling procedures for internal compliance, as the detriment to service members is significant.[112] While the study's findings do not specify how DCII training was flawed or how users misunderstood the purpose and proper use of data within the process, the study's silence on these issues only furthers the notion that there is not enough government transparency in the titling process. Without adequate disclosure of DCII training methodology and oversight or enforcement procedures, the barrier for relief is almost unattainable as the avenues to argue against the investigator's findings are already extremely limited. Unfortunately, requests submitted via the Freedom of Information Act ("FOIA") will often result in a stymie from the government agency through an avalanche of privilege or confidentiality assertions.[113] As stated by a former government employee who handled such requests, "[t]hese [federal FOIA departments] have no incentive to cooperate, and every minute they spend on tracking down documents is time taken from their actual jobs."[114] In short, Americans "have good reason to mistrust . . . attempts by agencies to fulfill requests."[115]

Stated plainly, the current version of titling falls well below the protections set forth in the Constitution because the very act of cataloging personal information in a database prior to establishing

112. *See id.* (noting that the Department of Defense "recommended several changes to DCII procedures to ensure that all users are initially, and periodically thereafter, informed of the DCII's purpose as well as the limitations concerning the content and use of criminal investigative data contained therein").

113. *See* Andrew McGill, *Why FOIA Is Broken, From a Government Worker's Perspective*, Atlantic (July 6, 2016), https://www.theatlantic.com/politics/archive/2016/07/why-the-freedom-of-information-act-is-broken-from-a-government-employees-perspective/623621/ [https://perma.cc/8EJB-9645] ("I've worked for state agencies, where nothing is more dreaded than FOIA duty. No one in the agency has the time to comply or has the slightest interest in doing so, because it is a tedious and unrewarding interruption to one's 'real' work and a terrible time suck. Everyone regards the FOIA people as an enemy . . . ."); *see also* Staff of H.R. Comm. on Oversight & Gov't Reform, 114th Cong., FOIA is Broken: A Rep. iii–iv (Comm. Print 2016), https://oversight.house.gov/wp-content/uploads/2016/01/FINAL-FOIA-Report-January-2016.pdf [https://perma.cc/CX5P-RP5Q] (finding, generally, that (1) the executive branch "encourages an unlawful presumption in favor of secrecy when responding to [FOIA] requests; (2) "[a]gencies overuse and misapply exemptions, withholding information and records rightfully owed to FOIA requesters"; (3) "FOIA requesters face agency roadblocks and struggle to decipher unclear communications from agency FOIA offices"; and (4) "[a]gencies create and follow FOIA policies that appear to be designed to deter requesters from pursuing requests and create barriers to accessing records").

114. McGill, *supra* note 113.

115. Staff of H.R. Comm. on Oversight & Gov't Reform, *supra* note 113, at iv.

probable cause may constitute an unreasonable search and seizure. First, the credible information standard, which allows a trained investigator to index someone in the DCII, is contrary to the probable cause standard safeguarded under the Fourth Amendment, which generally prohibits searches and seizures absent probable cause if there is a reasonable expectation of privacy.[116] Second, as discussed above, titling officials can still enter a service member into the DCII and establish probable cause at an unknown later date.[117] However, even while probable cause is pending, there is no mechanism to prevent adverse action or collateral consequences against the individual.[118] Absent probable cause, which was the former titling standard that had to be met in order to even index someone in the DCII,[119] the United States military arguably violates Fourth Amendment protections anytime a service member is entered into the database and information accessed by users. Generally, the Fourth Amendment applies to service members,[120] but only if there is an invasion of a legitimate expectation of privacy by the government.[121]

The applicability of the Fourth Amendment to service members, following an invasion of privacy, is supported by the United States Supreme Court's ruling in *United States v. Jones*, 565 U.S. 400 (2012), a case where law enforcement was found to have violated a suspect's Fourth Amendment rights after a GPS tracker was placed on his personal vehicle without a warrant. In that case, law enforcement tracked Mr. Antoine Jones for approximately a month

116. *See* U.S. Const. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . . .").

117. *See* U.S. Dep't of Army, *supra* note 92, at 29 ("A person or entity will be reported as the subject of an offense on the LER when credible information exists that the person or entity has committed a criminal offense.").

118. *See id.* at 29–30 (noting that a service member will not be removed from the DCII if there was credible information linking them to an offense, even if subsequent investigation that the allegation was unfounded).

119. Ham, *supra* note 87, at 6.

120. *See* United States v. Stuckey, 10 M.J. 347, 349 (C.M.A. 1981) (concluding that "'the Bill of Rights applies with full force to men and women in the military service unless any given protection is, expressly or by necessary implication, inapplicable' and, therefore, that the Fourth Amendment does shield the American service person") (citing United States v. Middleton, 10 M.J. 123, 126 (C.M.A. 1981)).

121. *See* Rakas v. Illinois, 439 U.S. 128, 143 (1978) ("[C]apacity to claim the protection of the Fourth Amendment depends . . . upon whether the person who claims the protection of the Amendment has a legitimate expectation of privacy in the invaded place.") (citing Katz v. United States, 389 U.S. 347, 353 (1967)).

and eventually arrested him in 2005 under suspicion of drug distribution.[122] The Supreme Court ultimately found the use of a warrantless tracking device constituted an unlawful search, and Justice Sotomayor's concurrence emphasized that Mr. Jones' property was usurped and his privacy invaded.[123] Five members of the Supreme Court classified the use of a warrantless GPS device as a search of Mr. Jones' property under the reasonable expectation of privacy doctrine, which is a two-part test that assesses whether there is a subjective and objective expectation of privacy.[124] In order to satisfy the test, the person must first have an actual subjective expectation of privacy and it must be established that society recognizes the expectation as objectively reasonable.[125]

While Military Rule of Evidence 314 permits the admission of evidence obtained from reasonable searches without probable cause, the standard has no bearing on a person's rights prior to the trial or court martial.[126] I argue that the placement of private information into the DCII or NCIC prior to probable cause being established, including any inquiry or search related to the entry, is an unreasonable search and that any detrimental impact stemming from the index constitutes an unreasonable seizure of property rights. Much like Mr. Jones' vehicle, his private property, was being tracked without a warrant, the United States military essentially utilizes the DCII and NCIC as a tracking device and houses sensitive information, without probable cause and warrant, in order to monitor service members.[127] Among other potential collateral consequences, an inquiry or search into the databases may qualify as unreasonable and may result in a seizure that restricts a service member's ability to travel (i.e., liberty), seek promotion or licensure (i.e., property interests), and even attend training schools or obtain benefits (i.e., educational and life

122. U.S. v. Jones, 565 U.S. 400, 402-3 (2012).

123. *Id.* at 413–14 (Sotomayor, J., concurring) (stating that in installing a GPS device on respondent's vehicle without a valid warrant, "[t]he Government usurped Jones' property for the purpose of conducting surveillance on him, thereby invading privacy interests long afforded, and undoubtedly entitled to, Fourth Amendment protection.").

124. *Id.* at 414 (Sotomayor, J., concurring); *id.* at 430 (Alito, J., concurring).

125. *Id.* at 414 (Sotomayor, J., concurring).

126. *See* Mil. R. Evid. 314(a) ("Evidence obtained from reasonable searches not requiring probable cause is admissible at trial when relevant and not otherwise inadmissible under these rules or the Constitution of the United States as applied to members of the Armed Forces.").

127. *See* Carpenter v. U.S., 585 U.S. 296, 305 (2018) (noting that Fourth Amendment doctrine cannot leave citizens "at the mercy of advancing technology" to preserve the same degree of privacy that existed when the Fourth Amendment was adopted) (quoting Kyllo v. U.S., 533 U.S. 27, 35 (2001)).

opportunities). It can be argued that, given the highly sensitive information that is potentially housed within the DCII and NCIC, there is an actual subjective expectation of privacy, especially when there is no finding of fault. There is also a general societal recognition that protecting private data is of utmost importance for the average citizen.

Overall, the titling process is a mechanism hidden from service members that may attach criminal stigma to someone without basic constitutional protections under the Fourth and Fifth Amendments. In its current form, it is a punitive system that does nothing but erode the rights and opportunities of current and former service members in perpetuity. Unfortunately, titling is not the only process currently attaching criminal stigma and depriving individuals of protected rights without basic constitutional protections.

### *B. Title IX Transcript Notations*

As discussed in detail in my initial publication, "Title IX of the 1972 Education Amendments prohibits sex discrimination in education programs and activities that receive federal financial assistance. While Title IX is an area of law that is now widely known, the scope of Title IX has metamorphosized over the years."[128] However, Title IX compliance was not effective until "the passage of the 1987 Civil Rights Restoration Act, . . . [which] required all academic institutions receiving federal financial aid . . . to abide by the requirements of Title IX" in all areas, rather than just areas where federal funding was received.[129] Arguably, the greatest changes to Title IX began to occur following

> the passage of the Jeanne Clery Disclosure of Campus Security Policy and Campus Crime Statistics Act ("Clery Act") in 1990, . . . [which] fostered the disclosure of information related to crime occurring on or around college campuses. While the Clery Act did not explicitly define what crimes had to be reported, it evidenced a clear intent by the federal government to address criminal conduct on campus . . . .[130]

128. *See* Cromartie, *supra* note 27, at 60 (citing Education Amendments of 1972, Pub. L. No. 92-318, tit. IX, 86 Stat. 235, 304–12 (1972)).

129. *Id.* at 61; *see also* Civil Rights Restoration Act of 1987, Pub. L. No. 100-259, 102 Stat. 28 (1988). This legislation was a concerted effort to reverse the effects of the Supreme Court ruling in Grove City Coll. v. Bell, 465 U.S. 555, 570–71 (1984), which held that only programs receiving federal financial assistance were required to abide by the requirements of Title IX.

130. *See* Cromartie, *supra* note 27, at 62 (first citing 20 U.S.C. § 1092; and then citing *Clery Act*, RAINN, https://perma.cc/VJ96-F8C4 (last visited Oct. 11, 2025).

On April 4, 2011, another drastic shift to the Title IX landscape occurred after President Barack Obama issued the first of several Dear Colleague Letters related to the handling of Title IX allegations on college campuses.[131] Since the issuance of the initial letter, postsecondary institutions increasingly investigated and litigated Title IX allegations.[132] However, Title IX has become a microcosm of political debate, as well as a source of private litigation, and seemingly changes with each new administration. While the most recent version of the Title IX regulations were enacted by the Biden administration on August 1, 2024, there is some uncertainty as to the finality of the proposed regulations as various states have initiated litigation to preclude enforcement of certain guidance.[133] Although litigation is ongoing, there does not appear to be a widespread dispute as to the general use of transcript notations in Title IX. However, with the reelection of President Donald Trump, further changes to Title IX may eventually occur.

Although transcript notations have been widely used by postsecondary institutions for decades, it was not until the Obama Administration's guidance that transcripts began to include notations arising out of Title IX disciplinary allegations.[134] Following the

131. Ali, *supra* note 25.

132. *See* Jeremy Bauer-Wolf, *A Look at 13 Years of Title IX Policy*, Higher Ed Dive (Apr. 22, 2024), https://www.highereddive.com/news/a-look-at-11-years-of-title-ix-policy/623810/ [https://perma.cc/9HQL-DV62] ("The 2011 [Dear Colleague] guidance is widely considered to be a catalyst for increased national attention on campus sexual violence.").

133. *See* Carnegie Mellon Univ., Fact Sheet: U.S. Department of Education's 2024 Title IX Final Rule Overview 5, https://www.cmu.edu/title-ix/university-response/files/t9-final-rule-factsheet-2024.pdf [https://perma.cc/YLF8-9J65] (last visited Sept. 10, 2025) (outlining the changes in the 2024 final rule); John W. Borkowski, Aleks Ostojic Rushing, & Noel Fisher, *Title IX Litigation Tracker: Where Do Things Stand Two Months After Implementation?*, Husch Blackwell (Oct. 1, 2024), https://www.k-12legalinsights.com/2024/10/title-ix-litigation-tracker-where-do-things-stand-two-months-after-implementation/ [https://perma.cc/ZWK7-ZME3] (citing the list of cases filed by a coalition of states challenging the new regulations).

134. *See* The Am. Ass'n of Collegiate Registrars & Admissions Officers, Transcript Disciplinary Notations: Guidance to AACRAO Members 7 (2017), https://www.aacrao.org/docs/default-source/signature-initiative-docs/disciplinary-notations/notations-guidance.pdf?sfvrsn=ecfe2557_0 [https://perma.cc/5TMB-AR6R] ("It has been common practice of registrars to record instances of suspension or dismissal due to low academic performance or substandard grade point averages . . . . Historically, many institutions even recorded notations of *academic* probation or warning on the official transcript."); *see also* Bauer-Wolf, *supra* note 132 (detailing how "the Obama administration first sought to use Title IX to bolster efforts to prevent campus sexual misconduct").

issuance of the Obama-era guidance, as well as a number of high profile cases where students transferred after being found responsible following a Title IX investigation, state legislatures around the nation began passing law that mandated the use of transcript notations.[135] The intent behind this legislation was largely to further the intent of the Clery Act by promoting public safety.[136] Essentially, Title IX transcript notations serve as a "quasi-criminal" record,[137] depending upon the nature of the allegations and [ultimate] disposition, that allows educational institutions, to document and track individuals who are found responsible of wrongdoing. The permanent nature and almost guaranteed adverse impact of a transcript notation has been the primary point of contention for those who oppose the notation process.[138] Essentially, opponents believe that such notations should not be utilized absent adequate protections and due process of law.[139] Depending upon school policies and pro-

135. *See Transcript Notations*, Advoc. For Youth https://knowyourix.org/issues/transcript-notations/ [https://perma.cc/58QE-XGD6] (last visited Feb. 24, 2024); *see also* N.Y. Educ. Law § 6444(6) (McKinney 2025) (requiring that, following a finding of responsibility for a violent crime (robbery, murder, motor vehicle theft, sex offenses, burglary, arson, etc.), schools place a notation on the student's transcript).

136. *See* Advoc. For Youth, *supra* note 135 ("Supporters of these efforts typically cite regulatory and safety concerns, arguing that, without transcript notations, offenders will transfer from school to school undetected. Alternatively, some survivors [of sexual misconduct], who feel that their lives have been forever altered by their assaults, support mandatory transcript notations in an attempt to ensure that their assailants suffer punishment just as long lasting.").

137. I refer to Title IX on-campus disciplinary processes generally as "quasi-criminal" in nature because the stigma attached to students who are found responsible can be significant. For example, if a student is found responsible for sexual harassment or assault and a notation is placed on his or her transcript, certainly there is criminal stigma attached to the individual. Further, Title IX disciplinary decisions are not bound by the burden of proof in criminal proceedings, which is beyond a reasonable doubt. In order to meet that burden in the criminal context, prosecutors must establish that there is no other reasonable explanation that can come from the evidence presented at trial. Instead, Title IX litigants are governed by lower civil standards of proof, such as preponderance of the evidence, which requires proving something more likely than not, or clear and convincing, which requires showing that the evidence is highly and substantially more likely than not to be true, depending on which iteration of Title IX regulations apply.

138. *See* Emma Ellman-Golan, *Saving Title IX: Designing More Equitable and Efficient Investigation Procedures*, 116 Mich L. Rev. 155, 175 (2017) ("[S]ome states like[ ]New York and Virginia . . . [have begun] to pass legislation requiring schools to note on a student's transcript whether the student was suspended or expelled for sexual misconduct, [and they] may face severe restrictions, similar to being put on a sex offender list, that curtail [their] ability to gain a higher education degree.").

139. *See* Fernand N. Dutile, *Students and Due Process in Higher Education: Of Interests and Procedures*, 2 Fla. Coastal L. J. 243, 254 (2001) ("In the context of higher

cedures, as well as state and federal law, educational institutions may have varying approaches to transcript notations.[140]

As briefly mentioned above, the primary debate regarding transcript notations centers around weighing public safety with individual due process rights and property interests. Where supporters laud notations as a form of recordkeeping that enhances public safety, critics of the mechanism fear that such notations may prevent any aggrieved individual from meaningfully pursuing a degree or employment, among other things.[141] Specifically, where criminal defendants enjoy a whole host of due process and procedural protections when facing allegations involving any crime, respondents who are accused of wrongdoing involving allegations of violence under Title IX face an uphill battle when defending themselves in on-campus proceedings as they are not afforded basic constitutional safeguards.

For example, where criminal defendants cannot be convicted of a charge until prosecutors establish each element beyond a reasonable doubt,[142] Title IX respondents can be found responsible simply

---

education, the threatened loss of an already-awarded degree presents the best case for procedural protection as 'property' under the Due Process Clause.").

140. For example, Virginia Commonwealth University's ("VCU") policy states that any student who is suspended, expelled, or withdraws while under investigation for an offense involving sexual violence will have a *prominent notation* placed on their transcript, subject to later removal or expungement. *Transcript Notations*, Va. Commonwealth Univ., https://dos.vcu.edu/student-resources-and-information/transcript-notations/ [https://perma.cc/V7H6-AED9] (last visited Sept. 10, 2025) (emphasis added). Pursuant to VCU's policy, a prominent notation "shall be substantially in the following form: '[Suspended, Dismissed, or Withdrew while under investigation] for a violation of [insert name of institution's code, rules, or set of standards].'"). *Id.*; *see also Policy and Procedure for Transcript Notations for Violent Crimes*, N.Y. Med. Coll., https://www.nymc.edu/policies/administrative-policies/transcript-notations-for-violent-crimes/ [https://perma.cc/3YNH-MA8F] (last visited Sept. 10, 2025) (indicating that students "who are suspended or expelled following a finding of responsibility for crimes of violence" or who withdraw while charges are pending will have a notation placed on their transcript without avenues for appeal or expungement for those who withdraw or are expelled).

141. *See The Important Issue of Transcript Notations*, Parisi, Coan & Saccocio, PLLC (Mar. 1, 2018), https://www.pandslawtitleix.com/blog/2018/march/the-important-issue-of-transcript-notations/ [https://perma.cc/J5CC-HCKY] ("In many cases these transcript notations can serve as a 'scarlet letter' of sexual assault or domestic/dating abuse and render it extremely difficult, if not impossible, for the marked individual to obtain desired employment or the continuation of his or her academic career.").

142. In order to convict someone of a crime, the finder of fact (i.e., the judge or jury) must find that the evidence presented was so convincing that no reasonable person could differ. *See Beyond a Reasonable Doubt*, Corn. L. Sch. Legal Info. Inst., https://www.law.cornell.edu/wex/beyond_a_reasonable_doubt [https://perma.

based on a preponderance of the evidence,[143] which has been described as "fifty percent [plus] a feather," a much lower standard, or by clear and convincing evidence.[144] Generally, criminal defendants are afforded greater protection due to the significant life, liberty, and property interests that may attach to any conviction. Where a criminal defendant may face incarceration, civil litigants, including those in Title IX proceedings, do not directly face such severe consequences. Yet, Title IX litigants, some of whom may face significant allegations, such as sexual assault, robbery, murder, or arson, among others, proceed without the same level of protection.

Although parties involved in the Title IX grievance process will never face imprisonment directly through that litigation,[145] the stigma that can be attached to someone found responsible for a Title IX allegation will be substantial, especially given that any finding of responsibility tied to crimes of violence must be reported pursuant to the Clery Act.[146] Additionally, the Title IX litigant still faces collateral consequences associated with any finding of responsibility, as well as potential parallel criminal proceedings. Further increasing the vulnerability of Title IX litigants is the potential for

---

cc/F7H8-K64R] (last visited Sep. 10, 2025) (defining beyond a reasonable doubt as "the legal burden of proof required for a criminal conviction," meaning that "the evidence must leave jurors firmly convinced of the defendant's guilt").

143. *See* 34 C.F.R. § 106.45 (2025) (permitting schools to use "the preponderance of the evidence standard of proof to determine whether sex discrimination occurred" in certain circumstances).

144. Whitener v. Sec'y Health & Hum. Servs., No. 06-0477V, 2009 WL 3007380, at *1 (Fed. Cl. Sept. 2, 2009); 34 C.F.R. § 106.45(h)(1) ("[T]he recipient must: (1) Use the preponderance of the evidence standard of proof to determine whether sex discrimination occurred, unless the recipient uses the clear and convincing evidence standard of proof in all other comparable proceedings, including proceedings relating to other discrimination complaints, in which case the recipient may elect to use that standard of proof in determining whether sex discrimination occurred.").

145. Meaning, Title IX respondents may still face criminal charges in a separate proceeding.

146. *See* 20 U.S.C. § 1092(f)(1). In relevant part, the Clery Act requires schools that receive federal funding to publish and circulate reports that disclose campus crime statistics. *Id.* Importantly, schools must report every criminal offense under the Act (homicide, murder, manslaughter, sexual assault, robbery, aggravated assault, burglary, hate crimes, motor vehicle theft, arson, hazing, Violence Against Women Act offenses, and drug, weapon, and liquor law violations) even if there is no ongoing investigation or finding of responsibility. *See The Jeanne Clery Act: Summary, Reporting Requirements, and Clery Center Resources*, Clery Center (last visited Dec. 3, 2025), https://www.clerycenter.org/the-clery-act [https://perma.cc/5RLC-U3HR]. Schools simply need to believe a potential crime was disclosed "in good faith" prior to reporting. *See* U.S. Dep't of Educ., The Handbook for Campus Safety and Security Reporting 4-10 (2016), https://www.ed.gov/sites/ed/files/admins/lead/safety/handbook.pdf [https://perma.cc/RFW8-WVND].

evidence and testimony introduced during the Title IX proceedings to be used in a parallel or subsequent criminal matter.[147] Another significant difference between criminal and Title IX proceedings is the requirement for a live trial or hearing. Where in the criminal realm defendants are entitled to a jury trial,[148] Title IX respondents are only afforded a live hearing before an individual decision-maker or a panel and may have to proceed virtually.[149] This mechanism is concerning for litigants as legal representation is not guaranteed and, if a litigant does not have an advisor present, the institution selects an individual to advise the individual.[150] Meaning, a party accused of robbery under Title IX, for example, may have to proceed to a virtual hearing where the respondent is not represented by an attorney and may have limited opportunity to assess or question the complaining party. Importantly, even if a party is found responsible for a Title IX violation, the individual will not be incarcerated unless an independent criminal investigation is initiated by government actors. For all intents and purposes, Title IX investigations are almost entirely internal.

Although Title IX proceedings are classified as administrative in nature, the stigma attached to an accused party can rise to the level of a criminal charge or conviction in the court of public opinion. Absent adequate procedural protections, Title IX litigants may not only experience disparate treatment associated with any stigma, they also may have their property rights impacted without due process.[151]

---

147. During a Title IX proceeding, a respondent may refuse to testify and assert privilege under the Fifth Amendment, which, in part, affords every citizen protection against self-incrimination, in order to avoid potentially introducing testimony that may have a negative impact on criminal proceedings. Absent the advice of legal counsel, or another legally trained individual, a Title IX litigant may not recognize this privilege, how to assert it, or when to assert it. *See Student Misconduct*, MATTHEW G. JUBELT, https://www.jubeltlaw.com/college-student-crimes [https://perma.cc/Q2RR-VZR7] (last visited Dec. 3, 2025).

148. U.S. CONST. Amend. VI ("In all criminal prosecutions, the accused shall enjoy the right to a speedy and public trial, by an impartial jury of the state and district wherein the crime shall have been committed . . . .").

149. *See* Nondiscrimination on the Basis of Sex in Education Programs or Activities Receiving Federal Financial Assistance, 85 Fed. Reg. 30026, 30053, 30069, 30370 (formerly codified at 34 C.F.R. § 106.45(b)(6)(i) and reinstated on Jan. 31, 2025), https://www.federalregister.gov/documents/2020/05/19/2020-10512/nondiscrimination-on-the-basis-of-sex-in-education-programs-or-activities-receiving-federal [https://perma.cc/8C2D-QPS2].

150. *Id.* at 30053, 30329 (formerly codified at 34 C.F.R. § 106.45(b)(5)(iv), (6)(i), and reinstated on Jan. 31, 2025).

151. *See* Mann, *supra* note 26, at 402 n.174 ("The Fourteenth Amendment's due process clause applies only to state action, meaning that only state schools, and not private schools, are covered by its requirements.") (citing Plummer v. Univ.

A few examples of property interests that may be jeopardized by the Title IX process may include, but are not limited to, the ability to pursue an education, employment, and now ownership of assets and intellectual property within the sports industry.[152] Under the Fifth and Fourteenth Amendments of the Constitution, federal and state governments cannot deprive any person of "life, liberty, or property, without due process of law."[153] Arguably, an individual's ability to pursue a degree in higher education, as well as one's reputation, implicates the life, liberty, and property interests under the aforementioned amendments. When analyzing what level of protection is required in such proceedings, courts generally turn to a three-factor analysis that requires the legal authority to determine: (1) What is at stake for the person?; (2) How risky is it that the person will be wrongly punished and how likely is it that more safeguards would reduce the risk?; and (3) How costly and time-consuming would the new protections be for the government?[154]

While the first and second factors certainly weigh in favor of a more robust system of protections for Title IX litigants, the third factor would hinge upon the nature and extent of any additional protections. In fact, prior to enacting former versions of the Title IX regulations, the Department of Education acknowledged potential costs and burdens that would be placed upon schools should procedures that are more robust be enacted, as is the government's responsibility when exploring proposed legislation.[155]

---

of Hous., 860 F.3d 767, 773 (5th Cir. 2017) (explaining that "due process requires notice and some opportunity for hearing . . . at a tax-supported college" (alteration in original))).

152. If a Title IX litigant is also a prolific student athlete, he or she may be entitled to rights and proceeds based on the individual's name, image, and likeness ("NIL"). Such NIL entitlements are likely subject to contracts with morality clauses that may be triggered by a Title IX accusation, thus potentially forfeiting a significant property interest.

153. *Id.* (citing U.S. CONST. amend. V, XIV).

154. *FIRE's Guide to Due Process and Campus Justice*, FIRE, https://www.thefire.org/research-learn/fires-guide-due-process-and-campus-justice [https://perma.cc/2Z3S-L2PT] (last visited Sept. 3, 2025); *see also* Mathews v. Eldridge, 424 U.S. 319, 335 (1976) (holding due process requires consideration of (1) the private interest affected by the official action; (2) the risk of an "erroneous deprivation" and probable value of additional procedure; and (3) the government's interest, including the fiscal and administrative burdens of additional procedures).

155. Nondiscrimination on the Basis of Sex in Education Programs or Activities Receiving Federal Financial Assistance, 89 Fed. Reg. 33474, 33483 (Apr. 29, 2024) (codified at 34 C.F.R. § 106 and rescinded on Feb. 4, 2025) ("The Department recognizes commenters' concerns that . . . aspects of the final regulations . . . will likely result in an increase in Title IX complaints for some recipients and possible additional administrative costs for some recipients.").

Although the Biden administration ultimately decided to remove live hearing requirements and the right to legal counsel, among other protections, it characterized these mechanisms as overly burdensome for schools.[156] My contention is that the cost and burden associated with any additional Title IX procedural protections is far outweighed by potentially hindering an individual's ability to pursue a degree, find employment, and maintain a sound reputation. Depending upon the nature of the allegations, once someone is accused of misconduct, the individual's information may be reported to law enforcement or campus safety that may store the information in a database, further compounding an individual's ability to participate in society long after the conclusion of proceedings (this is entirely dependent upon how the reporting party decides to proceed).[157] This is yet another example of a legally grounded process that contributes sensitive information to big data without adequate protection for the individuals involved in the legal proceedings.

As an exemplar on this issue in the realm of Title IX, I highlight the case of *Neal v. Colorado State University-Pueblo*.[158] In December 2015, Mr. Neal, an aspiring orthopedic surgeon at the time, was suspended from his academic institution and stripped of his wrestling and football scholarships during a Title IX investigation involving allegations of nonconsensual sexual intercourse, impeding his ability to pursue and obtain his degree.[159] The investigation was initiated after a roommate of Mr. Neal's partner reported that their sexual conduct was nonconsensual, which was contrary to representations from Mr. Neal and his partner, and was otherwise unsupported by third-party testimony. Mr. Neal and his partner even informed investigators of the consensual nature of the relationship.[160] Following Mr. Neal's suspension, a slew of online articles were published and his reputation tainted.[161] Although Mr. Neal filed suit against the

156. *Id.* at 33720, 33746–47.

157. *See* Ferguson, *supra* note 33, at 3 ("Government agencies collect health, educational, and criminal records . . . . Aggregating data centers sort and study the accumulated information in local and federally funded fusion centers.").

158. *See generally* Neal v. Colo. State Univ.-Pueblo, No. 16-cv-00873-RM-CBS, 2017 WL 11696393 (D. Colo. Sep. 11, 2017).

159. Complaint at 6, 32, 75, Neal v. Colo. State Univ.-Pueblo, 2017 WL 11696393 (D. Colo. Apr. 18, 2017). (No. 1:16CV00873).

160. *Id.* at 19–22.

161. *See id.* at 6 (alleging reputational harm suffered by Mr. Neal, including loss of educational, athletic, and career opportunities as described in the Prayer for Relief); *see also* Emma Gannon, *Judge Sees Bias in College Action Against Alleged Rapist*, Courthouse News Serv. (Feb. 21, 2017), https://www.courthousenews.

university and eventually entered a favorable settlement, the impact of the investigation is still being felt by him years after its conclusion. In fact, Mr. Neal, who is a professional mixed martial arts fighter,[162] has lost scholarships and other opportunities simply because he was publicly accused of sexual misconduct and suspended by the university.[163] Mr. Neal lost these professional opportunities because others discovered the articles related to his investigation online and perceived his suspension, which was viewed by the federal district court as improper, from the institution as an issue.[164] Importantly, Mr. Neal was suspended following a deficient Title IX investigation, as deemed by the court, during which the university did not provide a description of the allegations he faced, precluded Mr. Neal from presenting character evidence or witnesses in his defense, and utilized a single investigator who disregarded relevant, exculpatory evidence, but accepted subjective, hearsay evidence as true, among other issues.[165] Mr. Neal's experience highlights the importance of reviewing existing legal processes to ensure they are procedurally sound prior to exposing an individual to significant, long-lasting stigma. Had Mr. Neal initially been afforded a fair and equitable Title IX investigation, he may not have been suspended and may not have faced consequences stemming from online content and occurring years after he was absolved of the allegations. Undoubtedly, the widespread dissemination of the allegations against Mr. Neal via digital media and news outlets certainly exacerbated the consequences he faced. In all likelihood, the allegations against Mr. Neal will exist in perpetuity on the Internet.

---

com/judge-sees-bias-in-college-action-against-alleged-rapist/ [https://perma.cc/BM6D-HYEZ]; Robert Boczkiewicz, *CSU-Pueblo Files for Dismissal of Lawsuit*, Pueblo Chieftain (July 15, 2016), https://www.chieftain.com/story/news/education/2016/07/15/csu-pueblo-files-for-dismissal/9217977007/ [https://perma.cc/MVD9-ZYK6].

162. Ben Fowlkes, *A False Sex-Assault Claim Killed Grant Neal's Football Career, but MMA Provided a New Life*, Athletic (Aug. 22, 2019), https://www.nytimes.com/athletic/1155427/2019/08/22/a-false-sex-assault-claim-killed-grant-neals-football-career-but-mma-provided-a-new-life/ [https://perma.cc/EFG2-8PQD].

163. *See Former Football Player Sues School Under Title IX*, ESPN, https://www.espn.com/video/clip/_/id/17341553 [https://perma.cc/D9UQ-CNDR] (last visited Sept. 10, 2025).

164. *Id.*

165. *Id.*; Robby Soave, *Interview: This Male Student Was Expelled for Raping His Girlfriend Even Though She Said He Did Nothing Wrong*, Reason (Feb. 27, 2017) https://reason.com/2017/02/27/interview-student-expelled-for-rape-even/ [https://perma.cc/R83S-3AU6].

### *C. Law Enforcement Technology*

Arguably, the most far-reaching, rapidly developing, and hotly contested area of big data is the use of predictive technology,[166] which can be classified as person-based[167] or place-based,[168] by law enforcement. This data-centered, predictive approach to policing primarily originated in the 1990s after the New York City Police Department began regularly reporting statistics via a system known as CompStat and analyzing the data to adjust practices.[169] Since that time, predictive technology and its use has only continued to expand as billions of dollars in government funding and support from interest groups, such as police unions, has spurred its growth.[170] Much like the prior two processes, the debate concerning law enforcement technology

166. *See* Margaret Rouse, *Predictive Technology*, TECHOPEDIA (June 25, 2015), https://www.techopedia.com/definition/14525/predictive-technology [https://perma.cc/L9Z7-S8ZF] ("Predictive technology refers to a set of tools used for forecasting patterns in data while keeping in perspective the previous records/data.").

167. *See* Vahur Verte, *Person-Based Predictive Policing Under the AI Act*, ROBOTICS & AI L. SOC'Y (Apr. 20, 2024), https://blog.ai-laws.org/person-based-predictive-policing-under-the-ai-act/ [https://perma.cc/WMN9-VN97] ("Person-based predictive [policing] rests on the insight that negative social networks of individuals . . . can encourage criminal activity. It utilizes big data capabilities to develop predictive profiles of individuals based on past criminal activity, current associations, and other factors that correlate with criminal propensity.").

168. Tim Lau, *Predictive Policing Explained*, BRENNAN CTR. FOR JUST. (Apr. 1, 2020), https://www.brennancenter.org/our-work/research-reports/predictive-policing-explained [https://perma.cc/E37A-CLKK] ("Place-based predictive policing, the most widely practiced method, typically uses preexisting crime data to identify places and times that have a high risk of crime.").

169. James J. Willis, Stephen D. Mastrofski & David Weisburd, *Making Sense of COMPSTAT: A Theory-Based Analysis of Organizational Change in Three Police Departments*, 41 L. & SOC'Y REV. 147, 148 (2007).

170. *See* Andrew Guthrie Ferguson, *DOJ Funding Pipeline Subsidizes Questionable Big Data Surveillance Technologies,* THE CONVERSATION (Feb. 7, 2024), https://theconversation.com/doj-funding-pipeline-subsidizes-questionable-big-data-surveillance-technologies-222699 [https://perma.cc/78HS-DNUP] (highlighting the billions of dollars of federal funding given to law enforcement agencies to grow policing technology projects); *see also* Sarah Brayne, *Big Data Surveillance: The Case of Policing*, 82 AM. SOCIO. ASS'N 977, 981 (2017) (detailing how the federal government has heavily funded surveillance technology in local agencies); Patrick Yoes, Nat'l President Fraternal Ord. of Police, Testimony on Public Safety Communications in the United States, at 4 (Sept. 9, 2025), https://fop.net/wp-content/uploads/2025/09/testimony-20250909-subcomm-hearing-firstnet.pdf [https://perma.cc/XF7T-56P9] ("[I]ntegrating artificial intelligence (AI) . . . should enable even more sophisticated tools for public safety such as predictive analytics for threat detection and augmented reality for training."); *see also* Daniel DiSalvo, *Interest Groups, Local Politics, and Police Unions*, 11 INT. GRPS. & ADVOC. 263, 267–68 (2022) ("[Police unions] should be seen as key interest groups, as their leaders inevitably have influence on reforms touching on public safety and exercise power inside and outside of

and its use is primarily a balance between public safety and individual privacy rights. However, where an individual in military titling and Title IX proceedings is generally suspected of committing wrongdoing prior to being entered into big data, such may not be the case with technology maintained by law enforcement.

In fact, as briefly referenced above, the extent to which law enforcement collects information on citizens who have not committed a crime continues to increase as technology develops and avenues for data collection expand.[171] Where law enforcement entities once largely relied upon their own observations and investigative findings to populate records, police now have the ability to purchase consumer data from private companies, which permits law enforcement to cast a wide net that encompasses information associated with individuals who harbor no criminal record or suspicion.[172] Given the extent to which we rely upon technology on a daily basis, an individual's digital footprint[173] can be significant and, depending upon the data that is mined by law enforcement, could tell police your shopping habits, personal preferences, dietary restrictions, routines, or locations you frequent.[174]

---

city government . . . Evidence suggests that police unions have the resources to be important organizations shaping electoral politics.").

171. Currently, law enforcement utilizes a variety of information collecting devices, including, but not limited to, facial recognition, license plate readers, fingerprinting, aerial and social medial surveillance, etc. These data collection tools are subject to malfunction or less-than-optimum functioning, which can result in inaccurate data being entered into databases.

172. *See* Joshua L. Simmons, *Buying You: The Government's Use of Fourth-Parties to Launder Data about "The People,"* 2009 Colum. Bus. L. Rev. 950, 951–54 (indicating that government actors purchase consumer information associated with social media accounts, emails, phone numbers, etc.).

173. Defined as the data remaining each time we electronically transact, post on social media, or use our cell phones, among many other things.

174. *See* Ferguson, *supra* note 33, at 7–8 ("Currently . . . widespread surveillance remains in the hands of for-profit companies, for the purpose of offering consumers convenience and choice. But law enforcement is interested too." (first citing John Kelly, *Cellphone Data Spying: It's Not Just the NSA*, USA Today (Dec. 8, 2013); and then citing Nicolas P. Terry, *Protecting Patient Privacy in the Era of Big Data*, 81 UMKC L. Rev. 385, 391 (2012))); *see also id.* at 9 ("The World Privacy Forum—a watchdog group on personal privacy—estimates that there are 4,000 different databases collecting information on us." (citing Herb Weisbaum, *Big Data Knows You're Pregnant (and That's Not All)*, CNBC (Apr. 9, 2014), https://www.cnbc.com/2014/04/09/big-data-knows-youre-pregnant-and-thats-not-all.html [https://perma.cc/XT24-39LG])); *see also id.* at 12–13 ("The United States Senate Commerce Committee detailed how big data companies like Acxiom claim to have information on over 700 million consumers worldwide with over 3,000 data segments for nearly every U.S. consumer. Another company, Datalogix, claims to have data on almost every U.S. household." (first citing Fed. Trade Comm'n, Data Brokers: A Call for Transparency and Accountability 8

All of this data, along with information presumptively stemming from regular law enforcement business, such as arrest records, convictions, warrants, etc., is housed in databases maintained at the local, state, and federal levels by dozens of government agencies, including, but not limited to, the Bureau of Alcohol, Tobacco, and Firearms ("ATF"),[175] Department of Homeland Security ("DHS"),[176] and National Security Agency ("NSA").[177] Once information is entered into a law enforcement database, regardless of the source, it is then received by a regional information sharing system, which promotes interconnectivity and collaboration among law enforcement databases and agencies.[178] Although law enforcement entities may take varying approaches to their analysis of data, one thing is clear: Law enforcement is at least partially relying upon information obtained via private processes to further their investigation and policing practices.[179]

Unfortunately, the existing privacy laws in the United States, such as the Health Insurance Portability and Accountability Act ("HIPAA")[180] or Financial Privacy Act ("FPA"),[181] do little to prevent law enforcement from exploiting private user data in other ways, which raises concerns about a more overarching practice by law enforcement: the collection of information for one purpose, such as consumer preference through online cookies, and the use of it

---

(2014); and then citing MAJORITY STAFF OF S. COMM. ON COMMERCE, SCI., & TRANSP., 113TH CONG., A REVIEW OF THE DATA BROKER INDUSTRY: COLLECTION, USE, AND SALE OF CONSUMER DATA FOR MARKETING PURPOSES 5-8 (Comm. Print 2013))).

175. *National Tracing Center*, BUREAU ALCOHOL, TOBACCO, FIREARMS & EXPLOSIVES, https://www.atf.gov/firearms/national-tracing-center [https://perma.cc/EBQ9-NY8J] (last visited Sept. 10, 2025).

176. *DHS/ICE/PIA – 015 Enforcement Integrated Database*, DEP'T HOMELAND SEC., https://www.dhs.gov/publication/dhsicepia-015h-enforcement-integrated-database-eid-criminal-history-information-sharing [https://perma.cc/RLW9-2A4S] (last visited Sept. 10, 2025).

177. *See* Siobhan Gorman, *NSA's Domestic Spying Grows as Agency Sweeps Up Data*, WALL ST. J. (Mar. 10, 2008), https://www.wsj.com/articles/SB120511973377523845 [https://perma.cc/6AGU-48P5] (explaining how NSA gains access to large amounts of data from private companies).

178. *See About the RISS Program: A Proven Resource for Law Enforcement*, REG'L INFO. SHARING SYS., https://www.riss.net/about-us/ [https://perma.cc/HCM9-262K] (last visited Sept. 10, 2025) (discussing how the Regional Information Sharing Systems (RISS) Program "provid[es] adaptive solutions and services that facilitate information sharing, support criminal investigations, and promote officer safety and wellness.").

179. *See infra* notes 192–94.

180. *See* 45 C.F.R. § 164.512(f) (2025) (outlining circumstances in which "a covered entity may disclose protected health information for a law enforcement purpose").

181. *See* 12 U.S.C. §§ 3401–23 (2025) (permitting financial records to be disclosed for law enforcement purposes in various circumstances).

for a separate, potentially completely unintended purpose, such as predicting crime.[182] In fact, studies have already shown that law enforcement technology sometimes relies upon inaccurate data, leading to false arrests and other detrimental impacts, especially upon communities of color.[183] For example, FBI records have been shown to contain thousands of inaccuracies.[184] Yet, the accuracy and scope of information relied upon by law enforcement databases is not the only pitfall of the process.

The lack of transparency by law enforcement in terms of how their technology operates, what information they rely upon, the source of populating information, who is cataloged within the systems, and what oversight or safeguards are in place to ensure proper operation of the technology, are all issues fueling the debate around predictive technology. While still in its infancy, predictive technology in law enforcement has already resulted in flawed outcomes that have damaged public perception of the processes.

For example, the City of Chicago once relied upon crime data to generate a "heat list," which cataloged thousands of individuals who were viewed as potential future violent offenders.[185] Once identified on the heat list, police would visit an individual's home and notify them of their inclusion. Although Chicago police purportedly relied upon a variety of data to populate its heat list, the predictive technology sometimes identified individuals with no criminal record or police contact as at-risk individuals.[186] Ultimately, the use of heat

182. *See* Jon D. Michaels, *All the President's Spies: Private-Public Intelligence Partnerships in the War on Terror*, 96 Cal. L. Rev. 901, 901–05 (2008) (discussing "the Executive's apparent practice of identifying and then courting private actors, persuading, coaxing, and sometimes deceiving them to enter 'informal' intelligence-gathering" partnerships).

183. *See* Tim Cushing, *How Predictive Policing Got a Chicago Man Shot Twice*, Techdirt (June 3, 2021), https://www.techdirt.com/2021/06/03/how-predictive-policing-got-chicago-man-shot-twice/ [https://perma.cc/PQH2-9C98] (discussing the story of Chicago resident who was placed on a "heat list" and became the victim of gun violence because his interactions with police officers gave him a "snitch reputation").

184. *See* U.S. Dep't of Just., The Attorney General's Report on Criminal History Background Checks 26 n.20 (2006), https://bjs.ojp.gov/sites/g/files/xyckuh236/files/media/document/ag_bgchecks_report.pdf [https://perma.cc/L4AJ-H36H].

185. Monica Davey, *Chicago Police Try to Predict Who May Shoot or Be Shot*, N.Y. Times (May 23, 2016), https://www.nytimes.com/2016/05/24/us/armed-with-data-chicago-police-try-to-predict-who-may-shoot-or-be-shot.html [https://perma.cc/GP3E-PBF6]; *see also* Cushing, *supra* note 183.

186. *See* Ferguson, *supra* note 33, at 34 ("As a young man in Chicago, due to your friends, associates, and prior connection to violence, you have been predicted to be the . . . perpetrator of a shooting.").

lists was discontinued in 2019 due to sporadic results and imprecise methodology[187]; however, Chicago police still utilize other place-based predictive technology, which, as discussed below, carries with it its own issues.[188] Chicago's lack of transparency surrounding the formulation of heat lists is a common approach by most law enforcement entities that use technology. Often, law enforcement relies upon private third parties to provide the technology and code, which is protected as privileged, proprietary, or otherwise confidential information under intellectual property law.[189] Thus, the disclosure of algorithms or other processes used in furtherance of predictive technology may prove to be largely elusive and unattainable, even when utilizing FOIA or similar state record request procedures.

This general lack of adequate disclosure and transparency further complicates public trust in place-based predictions as historical data may increase the risk of technology targeting communities of color more than other populations, further exacerbating preexisting, racially grounded information.[190] As one scholar observed, "if the data is biased to begin with and based on human judgment, then

187. *See id.*; Jessica Saunders, Priscillia Hunt & John S. Hollywood, *Predictions Put into Practice: A Quasi-Experimental Evaluation of Chicago's Predictive Policing Pilot*, 12 J. Experimental Criminology 347, 363–66 (2016).

188. *See* Matt Straud, *Heat Listed*, The Verge (May 24, 2021), https://www.theverge.com/c/22444020/chicago-pd-predictive-policing-heat-list [https://perma.cc/4E36-T9ZT] (discussing how Chicago's predictive policing program led to a man being shot twice).

189. *See* Rachael King, *IBM Analytics Help Memphis Cops Get "Smart,"* Bloomberg Businessweek (Dec. 5, 2011), http://www.businessweek.com/technology/ibm-analytics-help-memphis-cops-get-smart-12052011.html [https://perma.cc/8M9N-6S46] (discussing cities' planned investments in policing technology and the consequent benefits for private companies).

190. *See* U.S. Sent'g Comm'n, Demographic Differences in Federal Sentencing 4 (2023), https://www.ussc.gov/sites/default/files/pdf/research-and-publications/research-publications/2023/20231114_Demographic-Differences.pdf [https://perma.cc/VBT8-W83Z] ("Black males received sentences 13.4 percent longer, and Hispanic males received sentences 11.2 percent longer, than White males."); *see also Criminal Justice Fact Sheet*, NAACP, https://naacp.org/resources/criminal-justice-fact-sheet [https://perma.cc/BVF3-VLLG] (last visited Sept. 4, 2025) ("A Black person is five times more likely to be stopped without just cause than a white person. . . . On average, Black Americans are exposed to four police killings of other unarmed Black Americans in the same state each year."); Sylvia Moreno, *Race a Factor in Texas Stops*, Wash. Post (Feb. 24, 2005), https://www.washingtonpost.com/archive/politics/2005/02/25/race-a-factor-in-texas-stops/b0317d23-7bf4-4cfc-b043-54d79d70e570/ [https://perma.cc/ZB3F-MNQE] ("[P]olice throughout Texas stop and search [B]lack and Latino drivers at higher rates than whites but . . . officers are more likely to find drugs, guns and other contraband on whites . . . . [O]verall, the statistics show a pattern of racial profiling.").

the results the algorithm is going to spit out will reflect those biases."[191] "In fact, those discriminatory data patterns will train the algorithms for future predictions, further obscuring the underlying bias. Race distorts judgment."[192] Predictive technology utilized in Florida from 2013–2014 has already been shown to have harbored racial bias after a study revealed Black criminal defendants were assessed to be high risk nearly twice as often as Whites purely based on the composition of data fed into the technology.[193] Results were skewed even after isolating "the effect of race from criminal history and recidivism, as well as from defendants' age and gender."[194] The central issue with such technology is that "in many U.S. cities, issues of race are bound up with issues of place. By law, practice, and custom, neighborhoods have been segregated by race and class."[195]

Regardless of the type of predictive technology utilized by law enforcement, there is one flaw that remains constant: human input. Both person- and place-based predictive technologies rely upon some sort of human interaction, in terms of data input or maintenance, in order to function.[196] While it is clear that humans must interact with data, maintain systems, analyze information, and run search queries, every human naturally harbors implicit biases[197] and other, potentially unrecognized, sentiments towards certain populations. Although human oversight is vital to ensuring proper functioning of technology, injecting human considerations, or any other information an individual believes to be relevant, into a digital process that is supposed to be impartial contaminates the analysis with

191. Bryan Llenas, *Brave New World of 'Predictive Policing' Raises Specter of High-Tech Racial Profiling*, Fox News (Jan. 11, 2017), https://www.foxnews.com/world/brave-new-world-of-predictive-policing-raises-specter-of-high-tech-racial-profiling [https://perma.cc/A88Y-RP2X].

192. Ferguson, *supra* note 33 at 49.

193. Julia Angwin et al., *Machine Bias*, ProPublica (May 23, 2016), https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing [https://perma.cc/W3SY-LNHC].

194. *Id.*

195. Ferguson, *supra* note 33, at 75.

196. *See* Irving Wladawsky-Berger, *Why Human Input Matters to Generative AI*, Medium (Oct. 4, 2023), https://medium.com/mit-initiative-on-the-digital-economy/why-human-input-matters-to-generative-ai-0ed1507fceb2 [https://perma.cc/9VDB-TSG3] (""Generative AI models need to train on human-produced data to function. When trained on model-generated content, new models exhibit irreversible defects.").

197. *See* Harini S. Shah & Julie Bohlen, *Implicit Bias*, StatPearls (Mar. 4, 2023), https://www.ncbi.nlm.nih.gov/books/NBK589697/ [https://perma.cc/S9G7-S3RX] (describing implicit bias as "the subconscious feelings, attitudes, prejudices, and stereotypes an individual has developed due to prior influences and imprints throughout their lives").

potential animus.[198] Complicating the potential fallout from any improper human input is the fact that "[i]ndividuals are unaware that subconscious perceptions, instead of facts and observations, affect their decision-making."[199] While proponents of predictive technology argue the process actually mitigates any human error or perception, prior studies have shown that error still occurs within these digital processes because of how law enforcement classifies or characterizes inputs and information when operating databases.[200] As one federal circuit court judge succinctly stated, "[g]arbage in, garbage out. Everyone knows that much about computers: you give them bad data, they give you bad results."[201]

Inaccuracies in such complex technology are bound to occur. We see error messages on a daily basis as we interact with much simpler media, such as social media platforms, routine Internet searches, and government-sponsored applications (such as utilities, student loans, or healthcare media). However, without a process to control quality and auditing and oversight mechanisms to address technological and human issues, error will continue to occur and impact lives. Given the interaction between humans and predictive systems, oversight and auditing must be performed regularly on not only the technology, but also its human operators. The FBI has already fallen prey to inadequate oversight after it was determined that their facial recognition technology, which contained facial images of seventeen million individual Americans, was not adequately evaluated for accuracy, leading to public outrage, false identification of potential

198. *See* David C. Vladeck, *Consumer Protection in an Era of Big Data Analytics*, 42 Ohio N.U. L. Rev. 493, 495 (2016) ("Algorithms may also be imperfect decisional tools. Algorithms themselves are designed by humans, leaving open the possibility that unrecognized human bias may taint the process. And algorithms are no better than the data they process, and we know that much of that data may be unreliable, outdated, or reflect bias.").

199. Shah & Bohlen, *supra* note 197.

200. *See* David N. Kelley & Sharon L. McCarthy, The Report of the Crime Reporting Review Committee to Commissioner Raymond W. Kelly Concerning CompStat Auditing 5–6 (2013), https://www.nyc.gov/html/nypd/downloads/pdf/public_information/crime_reporting_review_committee_final_report_2013.pdf [https://perma.cc/NN6R-YF6K] ("Reports in 2010, now substantiated, of the efforts of commanding officers . . . to downgrade and suppress the reporting of crime . . . cast further doubt in . . . the accuracy of the NYPD's numbers . . . . Police unions also have alleged widespread manipulation of crime statistics . . . . Precinct commanders purportedly induce, by threats or incentives, their subordinate[s] . . . to downgrade crime or not to take or file complaint reports in order to avoid criticism at CompStat meetings.").

201. U.S. v. Esquivel-Rios, 725 F.3d 1231, 1234 (10th Cir. 2013).

offenders, and an overall diminishment in trust.[202] This lapse is especially concerning after considering the immense system of interconnected security cameras and other data surveillance devices within the United States that are capable of facial recognition.[203] Ultimately, in pursuit of public safety measures, we must ask, "can correlation replace causation when the underlying data remains imperfect?"[204]

The due process implications are clear, and predictive technology, as well as surveillance that captures information on individuals without a warrant and feeds it into databases, is a violation of the Fourth Amendment prohibition against search and seizure. As referenced above, data is frequently collected by law enforcement without probable cause and, at times, absent any suspicion of wrongdoing, which sometimes leads to unforeseen and unwarranted consequences. The issue reduces to a simple question: how much of our private and constitutional rights are we willing to concede in the pursuit of public safety? Under current law enforcement surveillance practices, which permit surveillance of citizens in public and the use of predictive technology, information and data from individuals without any history of criminal activity or interaction with law enforcement may be collected and used by law enforcement in the name of safety.[205] The lack of notice to individuals whose information

202. *See* U.S. Gov't Accountability Off., GAO-16-267, Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy 10 & n.23, 25–26 (2016), https://www.gao.gov/assets/gao-16-267.pdf [https://perma.cc/7LS4-23Q9] ("FBI officials stated that they have not assessed how often NGI-IPS face recognition searches erroneously match a person to the database (the false positive rate)."); *see also* Jake Laperruque, *Unmasking the Realities of Facial Recognition*, Project on Gov't Oversight (Dec. 5, 2018), https://www.pogo.org/analysis/unmasking-the-realities-of-facial-recognition [https://perma.cc/UJ84-7Z9S].

203. *See 3 of the US Cities Under the Heaviest Video Surveillance*, Kustom Signals, Inc., https://kustomsignals.com/blog/3-of-the-us-cities-under-the-heaviest-video-surveillance [https://perma.cc/N788-KUW9] (last visited Sept. 11, 2025) ("Currently there are approximately 2,626 cameras around New York City connected to the NYPD's network and more than 18,000 interconnected cameras in the city. . . . In addition to . . . cameras, [Chicago] also [has] thermal and license plate recognition . . . cameras, and cameras on police and fire boats, helicopters, SUVs, trailers and command vans, among others.").

204. Ferguson, *supra* note 33, at 119.

205. *See* Jenifer Warren, *Task Force on Policing Releases Comprehensive Collection of Data on U.S. Law Enforcement*, Council on Crim. Just. (Feb. 11, 2021), https://counciloncj.org/task-force-on-policing-releases-comprehensive-collection-of-data-on-u-s-law-enforcement/ [https://perma.cc/688W-4Z25]; Bennett Cyphers, *Inside Fog Data Science, the Secretive Company Selling Mass Surveillance to Local Police*, Elec. Frontier Found. (Aug. 31, 2023), https://www.eff.org/deeplinks/2022/08/inside-fog-data-science-secretive-company-selling-mass-surveillance-local-police [https://perma.cc/6CFX-Z8NS] ("[R]ecords . . . indicate that Fog [Data Science,

is included in any law enforcement system, as well as the lack of general transparency with the public in terms of surveillance practices, further complicate the matter in that avenues for relief, such as expungement or appeal, are guised and hidden. If we do not recognize the issue, how can we address it via appellate or other restorative processes?

Given the uncertainty of how big data may progress and how law enforcement may continue to use the technology, the constitutional and privacy implications are somewhat uncertain. However, it is clear that constitutional standards enacted prior to big data are not keeping up with the rapid development of technology, leading to more and more due process and constitutional violations. For example, the Fourth Amendment of the United States Constitution, in part, authorizes law enforcement actors who subjectively and reasonably believe criminal activity is afoot to stop an individual they suspect is facilitating illegal activity.[206] "Reasonable suspicion" is the term that was adopted long ago to solidify this standard.[207] Through the *Sokolow* ruling, law enforcement was given leeway to stop and search individuals without a warrant, so long as certain prerequisites were met.[208] As discussed more in depth below, the flexibility associated with the "reasonable suspicion" standard, combined with the wealth of data relied upon by law enforcement, creates a situation where law enforcement can potentially justify improper acts through data. The logic furthered by law enforcement is that data and analytics are devoid of human influence, which somewhat shifts fault or liability from the member of law enforcement to the technological processes. This logic, however, is heavily contested as some civil rights advocates view law enforcement databases or other technological investi-

---

a commercial data broker,] has past or ongoing contractual relationships with at least 18 local, state, and federal law enforcement clients . . . . Fog states that it does not collect personally identifying information . . . . But Fog allows police to track the location of a device over long stretches of time—several months with a single query—and Fog touts the use of its service for 'pattern of life' analyses that reveal where the device owner sleeps, works, studies, worships, and associates. This can tie an 'anonymous' device to a specific, named individual.")

206. *See* U.S. v. Arvizu, 534 U.S. 266, 273 (2002) ("[T]he Fourth Amendment is satisfied if the officer's action is supported by reasonable suspicion to believe that criminal activity 'may be afoot'. . . ." (quoting U.S. v. Sokolow, 490 U.S. 1, 7 (1989)).

207. *See* Sokolow, 490 U.S. at 12 (1989) (Marshall, J., dissenting) ("[A] a suspicion is not reasonable unless officers have based it on 'specific and articulable facts.'" (citing Terry v. Ohio, 392 U.S. 1, 30 (1968))).

208. *See id.* at 7 (majority opinion) ("[P]olice can stop and briefly detain a person for investigative purposes if the officer has a reasonable suspicion supported by articulable facts that criminal activity 'may be afoot,' even if the officer lacks probable cause." (quoting Terry, 392 U.S. at 30)).

gative methods as human-driven.[209] Much like everything else that is man-made, maintenance and/or some human input is required for these databases to properly function. For example, devices as small as smart phones regularly require a software update initiated by data engineers to ensure proper functioning.

The primary issue is that law enforcement actors now have ease of access to a plethora of information related to an individual prior to even setting foot on the scene of a potential crime. Through big data and predictive technology, law enforcement, who, prior to the implementation and use of such technology were required to largely rely upon individual observations and circumstances existing at the scene, now may obtain a comprehensive profile of an individual prior to setting foot on scene. The use of tablets or similar devices provides law enforcement with a means to access an untold wealth of information about an individual with a few taps of the finger. Again, an individual without any criminal record or interaction with law enforcement may still experience a situation where government actors are judging them based on information derived from public surveillance or acquired from consumer data purchased from a private third-party company. Consider the following: "If the government wishes to deprive us of life, liberty, or property, fair process is due. . . . How do you get off a secret list you did not know you were on? How do you challenge a list when you cannot know the criteria? . . . How do you ensure transparency and accountability with opaque data-driven systems?"[210] At present, the United States government is allowing our constitutional rights to be eroded in the name of public safety, without limit, and without adequate notice.

If left unchecked, individual citizens may suffer from the growing pains associated with all new technology. For example, in January 2020, Robert Williams was arrested outside of his residence after police claimed he was suspected of stealing several high-value watches from a local jeweler.[211] Law enforcement suspected Mr. Williams after the victim store owner produced a single, grainy still image from his security system and produced it to police.[212] Investigating officials then took the still image and utilized their own facial recognition software to explore potential matches.[213] Ultimately, the technology

209. *See, e.g.*, Madison Blevins, *When Dirty Data Leads to Dirty Policing*, 29 Rich. J. L. & Tech. 166, 168, 171 (2023) ("Dirty data stems from routine human error . . . .").

210. Ferguson, *supra*, note 33, at 53.

211. *Williams v. City of Detroit*, ACLU (Jan. 29, 2024), https://www.aclu.org/cases/williams-v-city-of-detroit-face-recognition-false-arrest [https://perma.cc/9F92-DA25].

212. *Id.*

213. *Id.*

identified Mr. Williams as a possible match based off a then-expired driver's license that was stored in their system.[214] Police then took the results from their facial recognition software and made certain omissions to the court regarding the software's accuracy, leading to a warrant being issued and Mr. Williams' eventual arrest.[215] After being taken into custody and confined in an overcrowded cell, Mr. Williams was eventually released after thirty hours.[216] Unfortunately, the trauma experienced by the Williams family, who was present at the time of his arrest, and Mr. Williams during his time in custody, as well as any reputational harm, cannot be undone by his release. Mr. Williams ultimately filed suit against the City of Detroit and in June 2024 reached a favorable settlement.[217] In relevant part, the settlement agreement between Mr. Williams and the City of Detroit requires all law enforcement representatives to support facial recognition technology with "independent and reliable evidence" and to train all representatives on the use of such technology and its associated risks.[218] This timely outcome emphasizes the importance of heavily regulating the proper use of technology implemented by law enforcement and the potential disaster that may ensue if such technology is misused or misrepresented by law enforcement. As recognized by the *Williams* decision, courts must begin to recognize and think critically about the use of technology and the influence of human actors who rely upon such processes throughout criminal investigations.

## IV.
## ANALYSIS AND POLICY PROPOSAL

Prior to proceeding with proposals for policy reform, I must recognize the importance and potential benefits of utilizing predictive technology to further law enforcement and public safety efforts. While there is significant risk in implementing half-baked data processes to law enforcement, as well as to other areas of society, there can be significant benefit should greater safeguards and oversight be enforced. As one scholar noted, "blue data"[219] can serve as a countermeasure to some of the adverse impacts stemming from

214. *Id.*
215. *Id.*
216. *Id.*
217. *Id.*
218. *Id.*
219. *See* FERGUSON, *supra* note 33, at 143–66 (referring to the process of utilizing and analyzing internal law enforcement data to improve "police effectiveness, reduc[e] police violence, and strengthen[] training and accountability").

the use of predictive technology in law enforcement. For example, every law enforcement entity could develop and implement a system that focuses on accountability by cataloging public and substantiated complaints associated with individual peace officers. Such a process would not only further accountability, it would also assist law enforcement in identifying more efficient, public-friendly practices. In fact, databases have already been developed to index such occurrences.[220]

Unfortunately, these systems currently suffer from some of the main ailments that plague predictive technology: accuracy and lack of universal implementation of such oversight processes.[221] Without a robust system to monitor, audit, or otherwise control the collection and use of data by law enforcement, the risk of these technologies being abused by bad actors or the potential for technology to yield inaccurate information is heightened. Certainly, it will take time to develop a uniform process by which we balance collection and use of individual data by law enforcement. As discussed below, we must stem the ever-increasing impact of technology upon legal processes until we develop robust safeguards. While there is significant utility in technology utilized by law enforcement,[222] the benefit will be largely negated absent more robust protections in existing legal processes, as well as heightened oversight and auditing mechanisms. As noted by one data privacy expert,

> predictive policing, especially anything that goes to the level of identifying and evaluating individuals, is no different than stop and frisk . . . . Law enforcement is just passing the responsibility for bias to a [data] model rather than the individual officer . . . .

220. *See, e.g.*, *Justice Department Launches National Law Enforcement Accountability Database*, U.S. Dep't of Just. (Dec. 18, 2023), https://www.justice.gov/opa/pr/justice-department-launches-national-law-enforcement-accountability-database [https://perma.cc/4SU9-62A3] (discussing the National Law Enforcement Accountability Database ("NLEAD"), a "centralized repository of official records documenting instances of misconduct as well as commendations and awards for federal law enforcement officers").

221. *See* Alexis Kenyon, *Colorado's Database to Track Police Officer Misconduct Is "Wildly Incomplete and Often Flat-Out Inaccurate*," KGNU (Oct. 26, 2023), https://kgnu.org/colorados-database-to-track-police-officer-misconduct-is-wildly-incomplete-and-often-flat-out-inaccurate/ [https://perma.cc/P7D9-AZXG] (describing an investigation which found that Colorado's database was not being actively maintained and "failed to report the vast majority of officer misconduct, disciplinary actions or officer decertification").

222. *See generally* Ashley Johnson, Eric Egan & Juan Londoño, Info. Tech. & Innovation Found., Police Tech: Exploring the Opportunities and Fact-Checking the Criticisms (2023), https://www2.itif.org/2022-police-tech-future.pdf [https://perma.cc/T3WB-8YDP] (discussing benefits of police technology and methods of risk mitigation).

> Regardless of the algorithm used to predict, the individuals [targeted by law enforcement] quite literally 'fit a description.'[223]

A description entirely formulated through technological processes.

It is also vital to recognize the importance of our own role in furthering the safe and ethical use of technology. We continue to sacrifice our own privacy via everyday technological practices by, for example, accepting cookies on websites and signing service agreements without adequate review, which only contributes to the civil death. On an almost daily basis, we, as citizens, sacrifice our privacy to big data by clicking "I agree" on long user agreements, consenting to the use of cookies and data collection by websites, or posting our most intimate details and moments on social media, among many other things. Until we recognize the exposure created through our own individual practices, technology will continue to impact us in unforeseen ways, and the following policy proposals will be for naught.

In its present state, big data in the criminal recordkeeping and law enforcement contexts may result in the erosion and deprivation of constitutional protections without adequate safeguards, oversight, and accountability. While people advance these technologies in an effort to increase public safety, they do not meaningfully address the means. Specifically, various legal processes currently used within our society are antiquated once we consider the influence of big data in such contexts and the potential collateral consequences imposed upon citizens. As discussed above, titling in the military, the use of Title IX transcript notations, and the reliance upon predictive technology by law enforcement are three specific examples of legally grounded processes that are not keeping pace with the rapid progression of technology or are otherwise contributing to the collection and storage of private information without due regard for individual rights. The crux of my proposal is simple: we need to strike a fine balance between furthering public safety and maintaining individual rights and protections. I believe this effort is comprised of a two-prong approach. First, we must reassess existing legal processes and potentially implement additional safeguards in light of the rapid development and integration of technology in the legal realm. Specifically, we should enact additional safeguards focused on protecting one's information from technology maintained by law enforcement, thus mitigating the potential windfall of any arbitrary

223. Telephone Interview with Eric Curwin, Co-Founder & Chief Tech. Officer, Pyrra Techs (Dec. 7, 2024); *see also* Blevins, *supra* note 209, at 178–80 (discussing how predictive policing can reinforce biases).

stigma attached to an individual. Next, we must enact robust policies and procedures that focus on oversight of technology, proper use of technology by human actors, and auditing, or any similar process that ensures the technology itself is functioning properly.

### *A. Strengthening of Existing Legal Protections*

As to the first prong, my primary contention is that the three legal and administrative processes addressed in this Article are exemplary in that they maintain deficient procedural protections prior to storing an individual's information in big data. The first process, military titling, generally occurs prior to any hearing or legal representation and is determined relatively early in the investigation.[224] Most importantly, an individual can be titled even if formal charges are not brought or the individual is ultimately found not guilty of a charge. In the eyes of the United States military, guilt or innocence does not matter so long as you are initially listed as the subject of an investigation. As mentioned above, titling information can affect a service member's ability to seek promotion, specialty training, and benefits, among other things.[225] In terms of additional safeguards, I believe we must explore the following: (1) guaranteed, substantive involvement and review by legal counsel prior to indexing in the DCII or NCIC; (2) greater transparency via affirmative advisements to service members that contain the definition of titling, a description of the process, potential implications, and avenues for relief or expungement; (3) more robust avenues for appeal, including lower thresholds for service members to expunge improper titling information, as well as mandated document production by government actors; and (4) a limitation on the scope of information that is collected on a titled individual such that the impact of any collateral consequence is mitigated until there is a finding of guilt (i.e., the information stored on an individual should be relevant and sufficiently limited to the scope of allegations or charges). These are all safeguards that are absent in the current titling process and will continue to disparately impact service members, especially those who

224. *See* L. Off. of Jocelyn C. Stewart, *supra* note 20 (explaining that titling occurs when an individual is named as a subject in a criminal investigation report).

225. *See A Clear Explanation of the Military Titling Process: What Happens After You're Titled?*, Nat'l Sec. L. Firm, https://www.nationalsecuritylawfirm.com/a-clear-explanation-of-the-military-titling-process-what-happens-after-youre-titled/ [https://perma.cc/9V5X-GCX3] (last visited Sept. 11, 2025) ("The titling process in the military is a critical event with long-term implications that can affect a service member's career, reputation, and future employment opportunities.").

come from minority populations.[226] Much like our public criminal justice system, race is a driving force when it comes to the veraciousness of investigations and the severity of sentencing.[227]

Moving onto the next legal process, the use of transcript notations in Title IX proceedings, which, again, potentially attaches significant criminal stigma to individuals who are alleged to have committed some wrongdoing on a college campus. Historically, postsecondary schools were required to create quasi-criminal records in relation to on-campus misconduct proceedings, which were typically absent basic due process protections, such as a guaranteed right to confront one's accuser (i.e., cross-examination) or the right to an attorney, among others.[228] Given the volatile nature of Title IX law, it is possible the regulations will revert back to that standard. After considering mandatory federal and state reporting requirements, as well as related inclusion in a law enforcement database, the potential collateral consequences attached to individuals can be substantial and life-altering, especially after considering that Title IX investigations may end up in the public eye via news stories, word of mouth, or even privately maintained databases that track or otherwise monitor allegations against students and faculty.

In order to counteract the potential collateral consequences stemming from the inclusion of data originating from Title IX proceedings in law enforcement technology, we should consider establishing more robust protections, such as adopting a higher burden of proof in order to establish responsibility, among many other potential protections. For example, rather than utilizing a preponderance of the evidence standard,[229] the lowest legal standard, we may consider

226. *See* Wentz, *supra* note 19, at 320–24 (describing the disparate impact of current titling procedures and arguing that current titling procedures result in disparate impact).

227. *See id.* at 320 ("[D]ata showed a 'clearly discernable disparity in disciplinary rates between [B]lack and [W]hite servicemen . . . . [N]ot only were Black Service members disproportionately placed in pre-trial confinement, but . . . the length of time spent in pre-trial confinement was, on average, five days longer than white Service members and was the longest of any racial group in the study." (second alteration in original)).

228. *See* Mann, *supra* note 26, at 384 ("[B]y the time of the 2020 Rule, schools were using a variety of models ranging from the nonadversarial route of having the case handled by a trained Title IX investigator to use of quasi-courtroom adversarial models.").

229. *See Preponderance of the Evidence*, Cornell L. Sch. Legal Info. Inst., https://www.law.cornell.edu/wex/preponderance_of_the_evidence [https://perma.cc/T384-XNZA] (last visited Sept. 11, 2025) ("Under the preponderance standard, the burden of proof is met when the party with the burden convinces the fact finder that there is a greater than 50% chance that the claim is true.").

using the higher civil standard of clear and convincing evidence, which requires the complaining party to establish the evidence is substantially more likely to be true than not.[230] This change would simply increase the burden required to place transcript notations or attach stigma, which would afford litigants greater protection prior to being subjected to potential collateral consequences. An alternative approach would be to address the language included in transcript notations such that it is explicit no criminal wrongdoing has been established through the Title IX process. We should also seriously consider whether other due process mechanisms, such as the right to cross-examine a live witness, the right to trained legal counsel, and the right to a live, in-person hearing, should be adopted to further mitigate the disparate impact of any allegations that may be housed in big data. Although the Biden administration's version of the Title IX regulations was largely devoid of any of the aforementioned considerations, they have since been rescinded by the Trump Administration.[231] However, as mentioned above, nothing is preventing another administration from reverting back to the Biden standards. As such, we must fully appreciate the potential implications tied to prior iterations of the Title IX regulations before enforcing yet another version of the law.

This Article shifts now to the final legal process, predictive technology utilized by law enforcement, which, again, largely relies upon human input and may incorporate inaccurate data that has been collected without permission or through third-party commercial interactions.[232] Essentially, law enforcement is collecting data on private individuals through various means; data that may attach criminal or other negative stigma to an individual without any sort of notice or advisement.[233] While the majority of the issues associated

230. *See* Colorado v. New Mexico, 467 U.S. 310, 316 (1984) ("In contrast to the ordinary civil case, which typically is judged by a 'preponderance of the evidence' standard, [the clear-and-convincing-evidence standard requires that a party] place in the ultimate factfinder an abiding conviction that the truth of [the party's] factual contentions are 'highly probable.'").

231. *See* Nondiscrimination on the Basis of Sex in Education Programs or Activities Receiving Federal Financial Assistance, 89 Fed. Reg. 33474, 33746–47 (Apr. 29, 2024) (codified at 34 C.F.R. § 106 and rescinded on Feb. 4, 2025).

232. *See generally* Lee & Chin-Rothmann, *supra*, note 85 (describing how law enforcement avoids Fourth Amendment problems by purchasing data collected by private companies).

233. *See* Sara Morrison, *Here's How Police Can Get Your Data — Even If You Aren't Suspected of a Crime*, Vox (July 31, 2021), https://www.vox.com/recode/22565926/police-law-enforcement-data-warrant [https://perma.cc/67HE-NKX9] (explaining how law enforcement obtains copious amounts of individuals' personal data from third parties, with limited to no notice).

with predictive technology can be addressed through more robust oversight and auditing regulations, policies, and procedures, which is discussed in detail below, enacting greater restrictions on public data collection by law enforcement can also curtail some of the issues plaguing these systems.[234] Ultimately, any law enforcement data collection and usage should be narrowed and specifically tailored to the needs of any law enforcement task, investigation, or initiative. Absent reasonable articulable suspicion in compliance with the Fourth Amendment, we should not arbitrarily store data on individuals simply because it may be of use in the future or may inform future practices. If we do not tighten the restrictions on law enforcement data collection and use, we are permitting those agencies to essentially build a playbook on every individual without limit.

### *B. Enacting Robust Oversight and Auditing Processes*

The second prong of my proposal focuses largely on greater regulation and oversight of big data in the context of law enforcement and criminal recordkeeping through consolidated legislation. While the United States has previously attempted to provide greater data privacy rights through the American Data Privacy and Protection Act ("ADPPA"),[235] the proposed legislation ultimately failed, partially due to opposition led by United States Senator Ted Cruz.[236] Still, even the proposed protections under the defunct law were still insufficient when compared to more robust legislation enacted by other global powers, such as the European Union's GDPR.[237]

234. Most importantly, we should prohibit law enforcement agencies from accessing or purchasing private data from third-party companies regardless of any potential implications upon efficiency. As argued above, these private companies are monetarily motivated (i.e., potentially biased), are not regulated heavily enough, and fail to update or ensure the accuracy of their data. Stated plainly, law enforcement does not need to collect or understand my preferences as a consumer in order to inform their practices. My purchase of fish oil on Amazon has no bearing on my propensity to commit crimes, nor does the transaction further any investigation.

235. American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022).

236. *See* Jedidiah Bracy, *Stakeholders React to Draft American Privacy Rights Act*, INT'L ASS'N PRIV. PROS. (Apr. 9, 2024), https://iapp.org/news/a/stakeholders-react-to-draft-american-privacy-rights-act [https://perma.cc/2KUU-KWRL] (chronicling Senator Cruz's opposition to the ADPPA).

237. *See* ANGELA POTTER ET AL., ONETRUST DATAGUIDANCE, COMPARING PRIVACY LAWS: GDPR V. ADPPA, https://www.dataguidance.com/sites/default/files/onetrust-dataguidance-comparing-privacy-laws-adppav-gdpr-report_0.pdf [https://perma.cc/LQ5A-RCMS] (last visited Sepr. 18, 2025); Council Regulation 2016/679, General Data Protection Regulation), 2016 O.J. (L 119) 55, 11 (EU) ("Processing of personal data relating to criminal convictions . . . shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law

For example, while the GDPR is a comprehensive, all-encompassing piece of legislation that prioritizes the privacy of every EU citizen, individually, the ADPPA focused mainly on data security with attention to the records themselves and played on a patchwork of many other data privacy laws dedicated to specific types of information, which resulted in a hodgepodge of regulations.[238] The main issue with this approach is that the EU can simply regulate and enforce the legislation under a single umbrella whereas an American may have to pursue action through several areas of law depending upon the nature of the data or interest implicated. Accordingly, my primary proposal is that the United States should consider consolidating data privacy laws into a single, comprehensive piece of legislation not only to simplify the law and make it more accessible, but also to consolidate the aforementioned patchwork of laws at the state[239] and federal levels. This will ensure uniformity in law and provide greater clarity to the public at large.

While former President Biden had signed an executive order that seeks to enhance safeguards related to data collection and sharing, the initiative appears to primarily be driven by American compliance with the GDPR in terms of trans-Atlantic information sharing;[240] meaning, the initiative benefits larger systemic interests rather than individual ones. While the Biden administration's action is a step in the right direction, the proposed changes still fall short of the protections afforded by the GDPR.[241] Interestingly, the executive

---

providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.").

238. *See generally* POTTER ET AL., *supra* note 237 (discussing the similarities and differences between the GDPR and the ADPPA). For example, the ADPPA did not clarify its territorial scope, while the GDPR maintains extraterritorial scope. The GDPR also details the level of protection required prior to transferring data, whereas the ADPPA did not explicitly discuss the issue. The GDPR further requires data handlers to maintain a record of their activities, while the ADPPA did not. *See id.* at 8, 28, 32.

239. *See, e.g.*, 2008 Ill. Legis. Serv. 95-994 (West); CAL. CIV. CODE §§ 1798.100-199 (West 2018); TEX. BUS. & COM. CODE ANN. § 17.50 (West 2005).

240. *See* Exec. Order No. 14,117, 3 C.F.R. 366, 367 (2025) ("Access to Americans' bulk sensitive personal data and United States Government-related data by countries of concern through data brokerages, third-party vendor agreements, employment agreements, investment agreements, or other such arrangements poses particular and unacceptable risks to our national security given that these arrangements often can provide countries of concern with direct and unfettered access to Americans' bulk sensitive personal data.").

241. Christopher Munoz, *Experts Say Data Privacy Executive Order is Important for National Security*, SYRACUSE UNIV. TODAY (Mar. 7, 2024), https://news.syr.edu/blog/2024/03/07/experts-say-data-privacy-executive-order-is-important-for-national-security/

order recognizes the national security risk of allowing foreign actors to obtain

> United States Government-related data to collect information on activists, academics, journalists, dissidents, political figures, or members of non-governmental organizations or marginalized communities in order to intimidate such persons; curb dissent or political opposition; otherwise limit freedoms of expression, peaceful assembly, or association; or enable other forms of suppression of civil liberties,[242]

but it fails to acknowledge that similar consequences may arise from law enforcement's collection of individual data.[243]

In pursuing a uniform, comprehensive piece of legislation, I turn my focus to what has been proposed as the American Privacy Rights Act of 2024 ("APRA").[244] Where the ADPPA and President Biden's order left off, the APRA continues and expands upon the prior proposed protections. Most notably, the APRA affords a number of significant protections to private citizens, including, but not limited to, strict data minimization[245] and a focus on regulating large data holders.[246] Under the proposed legislation, covered data, or protected information, includes "information that identifies or is

---

[https://perma.cc/QTY6-RLQV] ("[The order] allows federal agencies to regulate the transfer of data to 'countries of concern.' . . . '[T]his order strategically addresses the large-scale transfer of Americans' personal data to foreign countries of concern[] . . . mitigating the potential threats on Americans' privacy and data protection against international risks . . . .'").

242. Exec. Order No. 14,117, *supra* note 240, at 367–68.

243. *See* KUSTOM SIGNALS, *supra* note 203 (detailing law enforcement's large-scale use of surveillance and data collection).

244. American Privacy Rights Act of 2024, H.R. 8818, 118th Cong. (2024).

245. Kirk J. Nahra, Ali A. Jessani & Amy Olivero, *New Federal Privacy Bill Draft Hits Congress*, WILMERHALE: PRIV. & CYBERSECURITY L. (Apr. 19, 2024), https://www.wilmerhale.com/en/insights/blogs/wilmerhale-privacy-and-cybersecurity-law/20240418-new-federal-privacy-bill-draft-hits-congress [https://perma.cc/3XE3-J2WP] ("[C]overed entities . . . are prohibited from collecting, processing, retaining, and transferring personal data unless they meet the data minimization principle of 'necessary, proportionate, and limited to' to provision or maintenance of a service or communication, or a specific permitted purpose. This language is stricter than what is currently required for companies under current state comprehensive privacy laws.").

246. *Id.* (under APRA, "large data holders, defined as 'a covered entity that has $250 [million] in annual revenue and collects or processes the covered data of more than 5 [million] individuals,'" would be required to designate data security and privacy officers, annually certify "certain compliance practices, and annually conduct[] an algorithm impact assessment if it uses a covered algorithm that 'poses a consequential risk of harm,' and biennially conduct[] privacy impact assessments").

linked or reasonably linkable," alone or in combination with other information, to an individual or a device that identifies or is reasonably linkable to one or more individuals.[247] While this is certainly a necessary protection, its potential effect is lessened by an exception that permits the collection of inferences gleaned from public information, which is sometimes inaccurate but still relied upon when indexing information and populating algorithms.[248] For purposes of this Article, this exception is concerning as the permitted inferences that can be made are broad in scope.[249] Additionally, the APRA does not appear to act as a true umbrella for American data privacy laws and seemingly still allows space for states to develop their own unique data privacy laws.[250]

Still, the APRA is not without its potential benefits and is certainly a step in the right direction. In fact, it is highly encouraging that the Biden administration had made a push to further data privacy rights in general. Most notably, even with the aforementioned issues, the APRA seemingly adopts the GDPR's focus on the individual in several areas. First, the proposed legislation provides individual control over covered data, meaning a person, after submitting a request to an entity that harbors their information, may be afforded the opportunity to access the information, correct any inaccurate or

247. *Id.*

248. H.R. 8818 § 101(12)(B) (excluding "inferences made exclusively from multiple independent sources of publicly available information . . . ."); *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. Online 15, 41 (2019) (discussing how predictive policing systems trained on public data "from jurisdictions with proven problematic conduct cannot be relied on to produce valid results . . . .").

249. *See* H.R. 8818 § 101(12) ("The term 'covered data' means information that identifies or is linked or reasonably linkable, alone or in combination with other information, to an individual or a device that identifies or is linked or reasonably linked to [one] or more individuals . . . . The term 'covered data' does not include . . . inferences made exclusively from multiple independent sources of publicly available information, if such inferences . . . do not reveal information about an individual that meets the definition of the term 'sensitive covered data' with respect to the individual; and . . . are not combined with covered data."). Sensitive covered data tentatively includes data such as government-issued identifiers, for example, a social security number; health and genetic information; comprehensive financial account and card numbers or access codes and passwords; and certain biometric information. *Id.* § 101(49).

250. *See id.* § 116(g) ("[N]o provision of this section may be construed as altering, limiting, or affecting the authority of a State attorney general, the chief consumer protection officer of a State, or an officer or office of a State authorized to enforce laws applicable to covered entities or service providers to . . . bring an action or other regulatory proceeding arising solely under the laws in effect in such State.").

incomplete information, and potentially delete it.[251] Next, the legislation provides a mechanism for individuals to pursue legal claims for actual damages, injunctive relief, declaratory relief, and reasonable attorneys' fees and costs of litigation, which will certainly encourage data management entities to comply with the law as they not only face sanctions from the government, but potential civil damage claims by individuals.[252] My concern with perceiving civil causes of action as an avenue for adequate relief is that they are often expensive, stressful, and time-consuming for litigants, which may act as a barrier to justice, as it always has in our legal system. Therefore, legislators should also consider utilizing an optional mediation process prior to any parties pursuing litigation, which is similar to the dispute resolution process offered by the Equal Employment Opportunity Commission, for example.[253] Early mediation, if facilitated by mandatory pre-mediation disclosure of relevant, non-privileged or confidential documentation,[254] would afford all parties an opportunity to potentially resolve the dispute early and significantly reduce the cost of litigation.

However, the APRA, much like the GDPR, contains a blanket "permitted purpose" exception, which permits collecting individual data for purposes of "prevent[ing], detect[ing], protect[ing] against, investigat[ing], or respond[ing] to an imminent or ongoing public safety incident (such as a mass casualty event, natural disaster, or national security incident)," as well as "ongoing or imminent security incident[s] relating to network security or physical security, including an intrusion or trespass, medical alert or request for a medical

251. *Id.* § 105(a).

252. *Id.* § 117(a).

253. *See Mediation*, U.S. Equal Emp. Opportunity Comm'n, https://www.eeoc.gov/mediation-0 [https://perma.cc/UQ2R-SUCQ] (last visited Sept. 19, 2025).

254. I advocate for mandatory pre-mediation disclosures simply because, in my professional experience, parties are reluctant to share information prior to litigation simply because it may increase their exposure. Without a mandatory disclosure requirement, parties will likely only disclose information and documentation that is most favorable to their position. This lack of disclosure would prevent the other party from learning potentially relevant information and greatly hinder assessing the veracity of the claims and defenses. For example, under Colorado law, litigants in civil district court must serve initial disclosures within twenty-eight days of the "at issue date," the date each defendant has been served and/or filed a responsive pleading. Colo. R. Civ. P. 16(b)(1), 26(a)(1). Each party's initial disclosures must contain (1) a list of every individual who may have information relevant to the claims and defenses asserted in the matter; (2) a list and copies of all relevant documents that are not subject to some sort of privilege; (3) an itemization of potential damages; and (4) a privilege log indicating what documentation was withheld, including the privilege asserted. *Id.* 26(a)(1), (b)(5)(A).

response, fire alarm or request for a fire response, or access control."[255] This provision also appears to afford law enforcement significant breadth when storing information under the guise of public safety. The proposed legislation also appears to permit entities to collect and retain information to conduct market research, which is concerning as this may open the door for private companies to continue the collection of information and sale to law enforcement.[256] While it is unclear exactly how these proposed legislative provisions will be enacted, they are but a few of the concerning aspects of the law that may not adequately address concerns voiced in this Article. As such, a need still remains for additional legislation that will enforce restrictions on law enforcement, or any entity maintaining criminal record information or otherwise contributing to public safety, and expand upon the APRA.

## V.
## CONCLUSION

Civil death, a concept that was once borrowed from English common law, will experience a modern resurgence if left unmitigated. Since the founding of our nation, our society has recognized the tension between individual freedom and governance. In fact, during a now-famed dispute between the Pennsylvania General Assembly and the Penn family, the founding members of the colony, and now state, Benjamin Franklin voiced a position that seemingly has more relevance now than it did at the time.[257] During the discussion, Mr. Franklin stated, "those who would give up essential liberty, to purchase a little temporary safety, deserve neither liberty nor safety."[258] While Mr. Franklin was merely commenting on the appropriateness of levying taxes against individuals in order to further the safety of the territory,[259] his statement remains relevant in the modern context as we continue attempting to strike a fine balance between public safety and individual rights. Where Benjamin Franklin and other American colonists debated how to develop and secure a nation

255. H.R. 8818 § 102(d)(11)–(12).

256. *Id.* § 102(d)(6).

257. *See Ben Franklin's Famous 'Liberty, Safety' Quote Lost Its Context in 21st Century*, National Public Radio (Mar. 2, 2015), https://www.npr.org/2015/03/02/390245038/ben-franklins-famous-liberty-safety-quote-lost-its-context-in-21st-century [https://perma.cc/WDF8-F35C] (revealing that during the dispute, the state legislature considered taxing the Penn family to bolster the security of the fledgling nation, a move met with staunch opposition).

258. *Id.*

259. *Id.*

through taxation, which was viewed as an intrusion upon individual rights at the time, we find ourselves questioning how much we, as individuals, should sacrifice in furtherance of public safety.

There are undisputed benefits of utilizing technology to facilitate public safety and the efforts of law enforcement, but the development and influence of such technology upon existing legal processes is rapidly eroding existing constitutional safeguards such that individual rights and liberties are being voided without due regard. As demonstrated through the three legal processes discussed herein, the existing safeguards in our current legal system may be inadequate given the significant impact criminal or civil allegations may have on an individual should their information be entered into big data. Where findings of responsibility in the civil realm or guilt in the criminal once had a more finite, punitive impact on an offender's life, technology and big data are now resulting in collateral consequences that have much broader and long-lasting impacts. As such, we must focus on exploring more individual-based data privacy legislation, as well as systemic oversight, so that public trust is not undermined. Simple measures such as regular audits, dedicated compliance teams with specific timelines, greater transparency, sunset mechanisms, procedural standardization, and the development and ownership of technology by government actors, not third-party entities,[260] may further public trust and safety at the same time.

Our modern predicament can be aptly summarized as follows: "[a]nyone who believes that new benefits make [people] forget old injuries deceives himself."[261] History has shown how questionable law enforcement practices can affect countless lives and history will continue to repeat itself if big data is left unchecked.

260. This would ensure that law enforcement or other government actors do not have to rely on algorithms developed by monetarily interested third parties. Such a simple measure would ensure that the government is solely responsible for acquiring and analyzing data, updating it, and ensuring its processes and users are operating properly.

261. Niccolò Machiavelli, The Prince 30 (Peter Bondanella ed. & trans., Oxford Univ. Press 2005) (1532).