ANNUAL REVIEWS

Annual Review of Criminology

Criminal Record Stigma and Surveillance in the Digital Age

Sarah Esther Lageson

School of Criminal Justice, Rutgers University–Newark, Newark, New Jersey 07102, USA; email: sarah.lageson@rutgers.edu

ANNUAL REVIEWS CONNECT
www.annualreviews.org
• Download figures
• Navigate cited references
• Keyword search
• Explore related articles
• Share via email or social media

Annual Reviews. Guest (guest) IP: 172.56.161.251 On: Sat, 24 Oct 2026 22:38:42

Annu. Rev. Criminol. 2022. 5:67–90

First published as a Review in Advance on September 13, 2021

The *Annual Review of Criminology* is online at criminol.annualreviews.org

https://doi.org/10.1146/annurev-criminol-030920-092833

Copyright © 2022 by Annual Reviews. All rights reserved

Keywords

criminal records, technology, stigma, surveillance, punishment

Abstract

This review analyzes criminal record stigma and surveillance through the concept of digital punishment: the collection and widespread dissemination of personally identifiable data by the American criminal legal system and subsequent private actors. The analysis is organized into three parts: a descriptive account of the technological, legal, and social factors that have created mass criminal record data; a theoretical framework for understanding digital criminal records through stigma and surveillance theories; and an argument that contemporary criminal records constitute digital punishment, with emphasis placed on how digital records are disordered, commodified, and biased. I close by raising policy-relevant questions about the widespread disclosure and uses of criminal legal system data for extralegal purposes.

Downloaded from www.annualreviews.org. Guest (guest) IP: 172.56.161.251 On: Sat, 24 Oct 2026 22:38:42

INTRODUCTION

In 1979, the US Bureau of Justice Statistics (BJS) released a manual called "Privacy and Security of Criminal History Information" detailing a complex set of decisions regarding what types of and how to disclose records to the media and public (US Dep. Justice 1979). The report noted the tension between those who "believe that most, if not all, of the workings of the criminal justice process ought to be public and those who believe that only some parts of that process should be public" (US Dep. Justice 1979, p. 1). The BJS pointed to three distinct interests at play: "the public's interest in receiving sufficient information to effectively monitor and participate in the functioning of the criminal justice system; the defendant's interest in limiting the availability of embarrassing and stigmatizing information; and the criminal justice system's interest in limiting the availability of information that, if released, might undermine the system's effectiveness" (US Dep. Justice 1979, p. 1).

At the same time, government operations were rapidly changing through technological innovations in data collection, aggregation, and sharing through the nation's new "rapidly expanding computer networks" (Rempel 1986). Sociologists warned in 1986 that "we've got big, powerful computers collecting information about all of us, but no one's managing the data—how it's used, its accuracy" (Rempel 1986). The scale of both criminal justice system operations and technological capabilities soared over the next few decades. Mass incarceration (Western 2006), the expansion of probation and parole (Phelps 2020), and the rise of public order and broken windows policing not only expanded the reach of the carceral state (Kohler-Hausmann 2018) but created ever more vast troves of data that documented police stops, court proceedings, and criminal convictions. The advent of increasingly data-driven criminal justice system operations (Hannah-Moffat 2019) exponentially accelerated historical trends in criminal record keeping (Brackett 2020) and furthered the growing institutionalization of criminal background checking, private-sector data collection efforts, and advances in surveillance and prediction (Blumstein & Nakamura 2009, Bushway et al. 2007, Urban Inst. 2017).

Criminal record data dissemination efforts were also aided by a permissive legal environment providing criminal record data to the private sector (Corda 2016) and a social acceptance for "eternal" criminal labels (Jacobs 2015) that culminate in collective patterns of digital punishment (Lageson 2020) where nearly any interaction with the legal system becomes a permanent data point. These data are widely published on the Internet as a stigmatizing label that is leveraged against people in a variety of extralegal settings. Although criminal records were once viewed simply as an administrative record, their social value has transformed over time into an object that sorts, classifies, marks, and punishes people in areas of life beyond the criminal justice system and now includes myriad records that extend from booking photos taken during a brief arrest to details of sentences served decades ago.

Bought, shared, and mined across public and private sectors, criminal record data have also become a robust Big Data commodity (Lageson 2020). Private data brokers hold vast repositories of criminal legal system information: For instance, the Data Diver Criminal Index claims to contain nearly 500 million individuals, with more than 2 billion criminal records ranging across 1,400+ jurisdictions (**https://www.edatadivers.com/about.cfm**). The criminal background checking industry is expected to grow to a $5.46 billion industry by 2025, a rise from 2016's estimated $3.74 billion projection (Res. Mark. 2018). The private sector has considerably widened criminal records' form, function, and scope, raising questions about extralegal sources of labeling, stigmatization, and punishment.

Criminal record data also constitute the foundation for increasingly ubiquitous surveillance databases used within and outside of the criminal legal system (Slobogin 2017). Predictive policing, smart prosecution, risk-assessment algorithms, and private-sector data brokers use, share, and

integrate criminal record data to create a technologically mediated gaze (Logan 2018, Lyon 2007). Much more than a single piece of paper an employer might request from the state, criminal records now implicate their subjects into a vast data ecosystem well before a criminal conviction (Hu 2015). Although state-sanctioned records were historically utilized primarily for state-sanctioned surveillance, criminal record data are integrated into Big Data surveillance systems used for digital reputation scores and informal background checks and to measure and predict consumer behavior (Lageson 2020). These patterns suggest criminal record data are an increasingly integral part of the everyday surveillance of the public and private sectors.

Finally, the aggregation and release of digital records have fundamentally changed the nature of traditional criminal records. In particular, the ubiquity of arrest, nonconviction, and incorrect criminal records available on the Internet raises punishment-related questions. Although many would agree that state conviction records are acceptable to be used in legal and nonlegal institutional settings, these new forms of criminal records contribute to social, psychological, and civil punishments. Government and courts have largely viewed this as an unintended outcome of the public nature of American criminal records and the advent of new technologies, but research suggests that those who experience the release of their criminal records online report myriad punishment-like qualities associated with criminal record data disclosures (Clair 2021, Gurusami 2019, Lageson 2020).

This review first lays out the sociolegal and technical factors that have led to our current moment and then provides a theoretical and conceptual framework for understanding the benefits and harms of the dissemination and aggregation of digital criminal records. The following sections use theories of stigma and labeling to theorize the dissemination of records, then turn to surveillance and technology studies to analyze the aggregation of criminal records as a Big Data commodity that contributes to governmental and private-sector surveillance. The concluding section argues that digital punishment emerges as a specific outcome of digital criminal record keeping and closes by considering policy implications.

THE CREATION AND DISSEMINATION OF DIGITAL CRIMINAL RECORDS

Digital criminal records emerge from the various agencies that compose the justice system continuum. In daily operations, police departments, local jails, criminal courts, prisons, and probation offices organize their work through data that track arrestees, defendants, and incarcerated people as they are processed through the governmental channels that make up the criminal legal system. Although increasingly sophisticated software platforms and technologies for tracking individual-level data are ubiquitous across human services, government, and the private sector, data created about individuals processed within the criminal legal system are uniquely classified as a public record and released into the public sphere. These disclosures of personally identifiable information have contributed to the growing personal data and commercial background checking industry that relies on the availability and affordability of criminal record data (Conley et al. 2011, Kaspero & Canhasi 2018) and are disseminated across a suite of websites that offer people-search services, community notifications, and public data portals (Corda & Lageson 2020).

State criminal records are historically rooted in the Progressive era, when "proponents argued that an effective system of criminal record collection was part and parcel of the creation of a modern, scientific and efficient crime control system" (Brackett 2020, p. 156). A broad set of interests coalesced around the new institution of criminal record keeping, including the medical treatment model embraced by rehabilitationists and social workers, the increased police use of information to track suspects and conduct investigations, the desire to use criminal records as statistical data by early criminologists, and new punishment systems of marking and

Downloaded from www.annualreviews.org. Guest (guest) IP: 172.56.161.251 On: Sat, 24 Oct 2026 22:38:42

disenfranchising people newly labeled as "felons," particularly in the US South during Reconstruction (Brackett 2020).

In the modern punitive era of the 1970s to the present, criminal records became increasingly public through registration and community notification systems that share identifying information with the public at large (Logan & Prescott 2021, p. ix). The dominant assumption was that "there is no such thing as an 'ex-offender'—only offenders who have been caught before and will strike again. 'Criminal' individuals have few privacy rights that could ever trump the public's uninterrupted right to know" (Garland 2001, pp. 180–81). Records were institutionalized as markers of both risk and culpability (Lynch & Bertenthal 2016), became integral to employment and housing screening processes, and attached to a vast set of civil legal penalties in what became known as collateral consequences (Uggen & Stewart 2014).

Today, disclosing records to the general public is generally framed around public safety, government transparency, and First Amendment rights. Public criminal record repositories, such as sex offender registries, are used for both informational and punishment functions (Logan 2009), and criminal records as background checking tools are firmly entrenched in American institutional decision-making, where records are used to assess risk and exposure to liability or harm in the workplace, school, or community (McElhattan 2018). The criminal label may serve as a deterrent (Sherman 2014, Thomas & Bishop 1984, Ward & Tittle 1993); however, this has been debated in the criminological literature, particularly in light of the negative stigma of a criminal record (Pager 2007, Uggen et al. 2014) and the potentially criminogenic effects of labeling (Chiricos et al. 2007, Restivo & Lanier 2015).

Records are also seen as a mechanism to promote government transparency. Supreme Court Justice Louis Brandeis (1913) famously argued that "sunlight is said to be the best of disinfectants; electric light the most efficient policeman." In *Nixon v. Warner Communications, Inc.* (1978), the Supreme Court held the right "to inspect and copy public records and documents, including judicial records and documents." Common law and public policy have followed this spirit of openness, citing benefits such as protecting the accused from "unjust prosecution by public officials" and "instill[ing] a sense of public trust in our judicial process" (*Westchester Rockland Newspapers v. Leggett* 1979). Making the legal process public should, in theory, provide the public with a more complete understanding of the judicial system and a better perception of fairness (*Republic of the Philippines v. Westinghouse Electric Corp* 1991). Once disclosed by the government, digital records are mined, scraped, or purchased by third parties, who aggregate records into databases containing other types of personal data, or posted to websites or other online repositories (Lageson 2020). As publicly disclosed criminal records are duplicated across websites and databases, they are indexed into Internet search results, wherein a Google search for a person's name may yield dozens of websites that repost criminal record data (**Figure 1**). For instance, online mugshot galleries contain millions of booking photographs, searchable by name and city (Lee 2018), and hundreds of websites offer free or inexpensive access to public criminal record repositories. These practices are legal under First Amendment and government transparency laws.

Public opinion has shown support for disclosing certain types of records; nine out of ten respondents in a 2000 survey supported criminal record disclosure for employment or volunteering purposes (US Dep. Justice 2001). However, the same 2001 survey showed that 90% of respondents expressed concerns about the misuse of personal information in disclosed criminal records, and 90% of respondents preferred that state agencies do not use the Internet to post public criminal history information. In a survey nearly two decades later, the use of criminal records by private companies received similarly low support, where 88% of respondents opposed the publication of arrest records by private companies (Lageson et al. 2019). This research suggests a growing interest in privacy for criminal records; reformers also argue that government can, and perhaps should,

Downloaded from www.annualreviews.org. Guest (guest) IP: 172.56.161.251 On: Sat, 24 Oct 2026 22:38:42

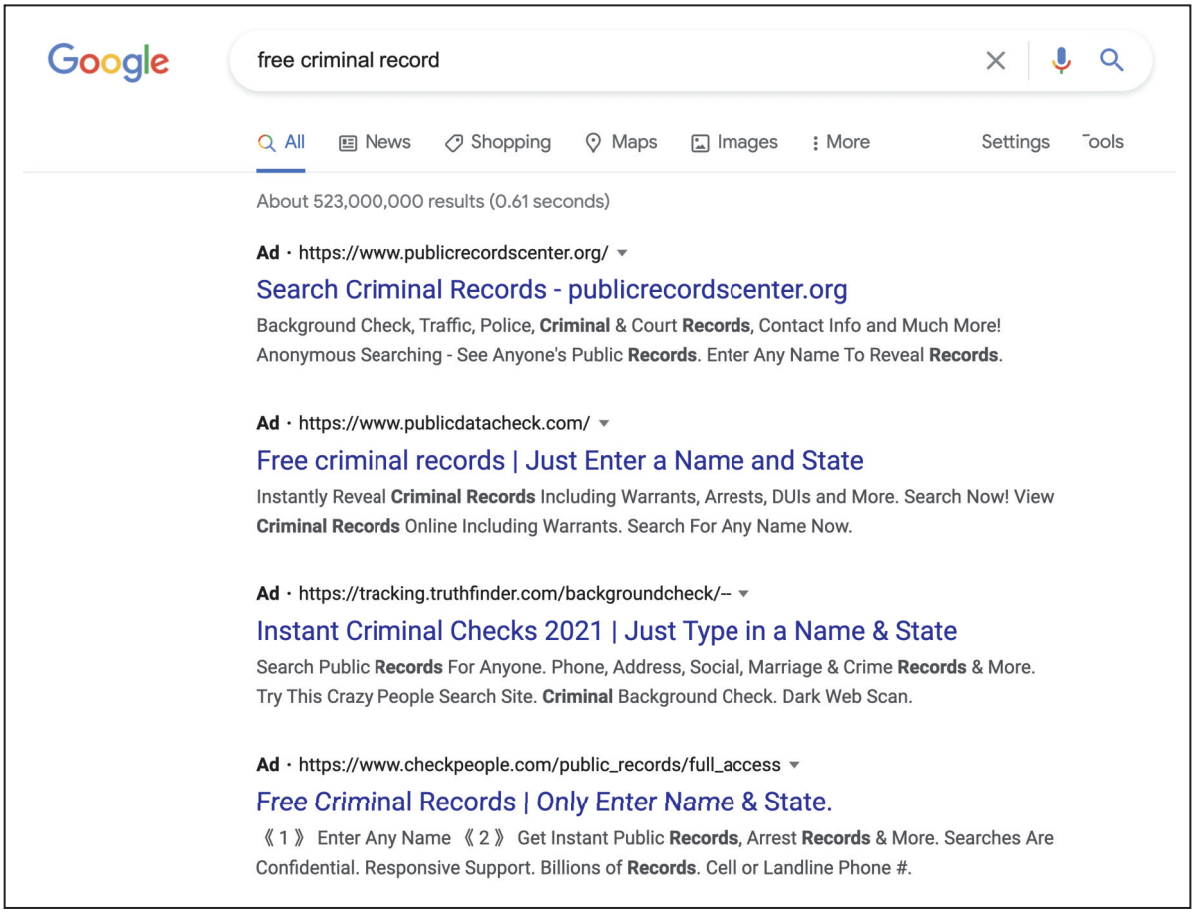

Figure 1

Screenshot of Google Search Results for companies offering criminal record services.

limit the types of personally identifiable information that is released into the public record and prevent bulk distribution for commercial purposes, including arrest and charging data that fail to show relevant case dispositions.

THEORETICAL FRAMEWORKS

The broad disclosure and aggregation of criminal records through digital platforms and databases raise theoretical and pragmatic questions about stigma, surveillance, and punishment through the criminal legal system. Although criminal record stigma has been extensively studied in criminology, the digital context allows for new interpretations of long-standing theories of how criminal record stigma operates, namely that criminal records now appear in multiple public and private formats. The ubiquity of police, court, and correctional records as part of a broader data ecosystem also invites new perspectives to conceptualize records as part of digital surveillance.

Criminal Record Stigma

Criminal records plainly attach stigma and its co-occurring parts: labeling, stereotyping, status loss, and discrimination (Link & Phelan 2001). Digital technology has altered and enhanced

Downloaded from www.annualreviews.org. Guest (guest) IP: 172.56.161.251 On: Sat, 24 Oct 2026 22:38:42

criminal record stigma in several key ways. First, the process of attaching the criminal label is no longer reserved for state actors only. Rather, a multitude of private actors can now magnify and publicize the criminal label or introduce it into a host of new spaces, such as social media and Internet search results. Records that sat undisturbed for decades might suddenly appear on the Internet or become widely public after being reposted to a private website optimized for search engine crawling (Lageson & Maruna 2018).

Second, the Internet provides a new forum for the expressive role of punishment and shaming, where online sources recodify the crime complex of modern times (Garland 2001), expanding the reach of public punishment. Digital records recenter crime into daily life, transitioning from being an item a person had to actively seek out in person at a courthouse to a bit of information one can inadvertently discover through a Google search.

Third, the endurance of digital labels poses problems for our understanding of desistance processes, which partially rely on the ability to move on from criminal record stigma through a variety of psychosocial processes and identity management strategies now interrupted by the eternal criminal record (Jacobs 2015). These technological shifts motivate a reconsideration of punishment and stigma that recognizes new dynamics for both the labeled and the labelers who harness the Internet to expose individuals accused of crimes (Lageson & Maruna 2018).

Historically, scholarly attention to stigma was largely initiated by Erving Goffman's seminal 1963 book *Stigma*, in which Goffman distinguishes between those who are discredited (whose stigma is visible or clearly known) and those who are discreditable (whose stigma can be concealed). Those with a discreditable stigma are concerned with stigma management: "To display or not to display; to tell or not to tell; to let on or not let on; to lie or not to lie; and in each case, to whom, how, when, and where" (Goffman 1963, p. 42). Criminal records get brief attention in Goffman's *Stigma*, reflecting a predigital era: "An ex-convict, for example, can only disclose his stigma widely by improperly presuming on mere acquaintances, orally disclosing to them personal facts about himself which are more personal than the relationship really warrants. A conflict between candor and seemliness will often be resolved in favor of the latter" (Goffman 1963, pp. 74–75). It is clear that today, people with criminal records are almost certainly within Goffman's category of the discredited, with an easily discoverable and highly visible stigma.

Stigma and labeling theories are also concerned with social reactions to deviant characteristics and negative credentials and the subsequent internalization of publicly applied labels through signification processes (Matza 1969) where labels are incorporated into a person's identity. In turn, desistance scholars argue that the interplay of identity and stigma holds repercussions for people's ability to move on from their pasts. Maruna (2001, p. 7) argues that to maintain "abstinence from crime, ex-offenders need to *make sense* of their lives" by developing a coherent identity for themselves. This "willful, cognitive distortion" is referred to as "making good" (Maruna 2001, p. 9). Those who have been successful in desisting from crime, Maruna writes, have developed redemption scripts by seeking to turn their past lives into something positive. Desistance has also been analyzed through the concept of cognitive transformations that are related to environmental "hooks for change" (Giordano et al. 2002) that allow for life-course transitions away from prior legal system involvements. The perpetuity of digital stigma may, however, limit opportunities to build redemption scripts or respond to hooks for change, hindering the cognitive and personal transformations necessary for desistance from crime.

Other researchers have analyzed external factors that contribute to unlabeling and desistance processes. Life-course research has suggested that the adoption of normative social roles, such as getting married or gaining stable employment, can help sustain the process of desisting from crime (Laub & Sampson 1993). As people grow up, move on, and proceed through the stages of their lives, they have opportunities to reconstruct new identities for themselves (Sampson &

Downloaded from www.annualreviews.org. Guest (guest) IP: 172.56.161.251 On: Sat, 24 Oct 2026 22:38:42

Laub 2003). The unexpected public disclosure of an arrest and the likelihood that the resulting criminal record will remain online can interrupt these processes; if a criminal record suddenly becomes known to employers, friends, potential partners, or family members, the self-fulfilling process of stigmatization might disrupt otherwise positive outcomes. For instance, one study of digital criminal record disclosure found an 11% increase in recidivism rates after local jurisdictions created online, public criminal record databases (Luca 2018). Qualitative work has shown how contemporary criminal record disclosures have led people to avoid the institutional arrangements crucial to desistance, or even react to overwhelming stigma with hopelessness or a turn back to criminal behavior (Lageson & Maruna 2018). In this sense, digital disclosure could prove to be criminogenic, but more research is needed to explore potential causal relationships.

Furthermore, inaccuracies in criminal record data may problematize our traditional understandings of labeling, stigma, and desistance, particularly when people are forced to contend with a wrongfully represented self through misleading criminal record data (Myrick 2013) or errors in criminal records (Lageson 2020). Decades ago, Goffman predicted the social-psychological consequences of such differential identities, warning that "a discrepancy may exist between an individual's virtual and actual identity. . . . This discrepancy, when known about or apparent, spoils his social identity; it has the effect of cutting him off from society and from himself so that he stands a discredited person facing an unaccepting world" (Goffman 1963, p. 19). Research is needed to understand the complex relationship between public criminal records, data quality, stigma durability, and desistance processes. There are, however, methodological barriers to this type of research, as criminologists have traditionally used a government-sanctioned criminal record label as the independent variable used to predict a broad variety of individual outcomes. How then might we measure the effects of digital labels that may derive from so many sources and show up in unexpected arenas?

Criminal Record Surveillance in the Digital Age

Since the late 1920s, criminal records have been integral to governmental surveillance efforts to combat crime (Brackett 2020). Today, criminal records are increasingly conceptualized and used as a source of data for predictive or algorithmic justice system operations or are aggregated into consumer, real estate, social media, and other sources of personal data, then repackaged into large data sets sold to public and private actors. Although criminal records themselves do not constitute a de facto surveillance device, Big Data approaches to criminal legal operations have increasingly transformed criminal records from an administrative tool used for internal state purposes to a piece of risk management information for extralegal actors (such as employers and landlords) and further to small bits of data aggregated into vast databases used to track, monitor, and predict human behavior. Today, the broad disclosure of criminal records to private data brokers and the Internet at large has broadly expanded what we might now think of as everyday surveillance.

An integration of surveillance and technology studies perspectives may aid our understanding of the role criminal record data play in contemporary society. Surveillance has been theorized as a mode of governance through macrolevel efforts of "sorting things out" (Bowker & Star 2000) that encourages self-discipline through oversight (Foucault 1977, Garland 1997) and, with the advent of computerization, creates a networked surveillance assemblage that spans institutional and social sectors (Lyon 2007, p. 4). Although surveillance, the "collection and analysis of information about populations in order to govern their activity" (Haggerty & Ericson 2006, p. 3), has long been a central concern in theories about modernity, global capitalism, labor, and governmentality, the dramatic rise in the sheer size of the American criminal justice system has centered

Downloaded from www.annualreviews.org. Guest (guest) IP: 172.56.161.251 On: Sat, 24 Oct 2026 22:38:42

police, courts, and prisons as key sites of data collection and surveillance (Brayne 2014). A broad body of research on the intersection between surveillance and the legal system has focused on the magnitude and scale of surveillance through mass penal systems, the surveillance inequalities reproduced through criminal record data aggregation, and responses to surveillance through avoidance, disengagement, self-surveillance, and legal estrangement.

The expansion of the criminal justice system developed alongside the growth of digital technologies used to administer and organize the growth of Big Data analytics. Criminal records, as one key data source, are the building blocks of surveillance systems that extend both inside and outside the legal system. Nearly one-third of the US population has some type of criminal record (Sentencing Proj. 2014). Among the general population, 19.8 million people are estimated to have a felony conviction (Shannon et al. 2017). A full 30% of US youth have an arrest record by age 23 (Brame et al. 2012), with risk unevenly distributed by race and gender (Brame et al. 2014). The state itself originates this surveillance through the voluntary release of criminal record data to the public and private sector; estimates show that approximately 10.16 million digital arrest records are published on the Internet each year by local police departments, culminating into more than 101 million records over a decade. Approximately 4.57 million mugshots are released annually, culminating in more than 22.8 million mugshots in five years (Lageson et al. 2021).

The wide availability and ease of aggregating criminal and other types of personal data have accelerated the drive toward smart, data-driven, and evidence-based criminal legal operations (Hannah-Moffat 2019). Although these efforts are often framed within public safety and crime prevention strategies, "big data technologies can be used for high-tech profiling of people, events and places; they can violate constitutional protections, produce a false sense of security and be exploited for commercial gain" (Hannah-Moffat 2019, p. 465). The mass collection of criminal record data has concerned scholars who critique these widespread data surveillance efforts as marking individuals with digital suspicion through Big Data blacklisting (Hu 2015), creating systems of algorithmic injustice that reflect and reproduce inequities but are "promoted and perceived as more objective or progressive than the discriminatory systems of a previous era" (Benjamin 2019, p. 3). Although criminal records were initially created to manage internal criminal justice agency operations, the aggregation and disclosure of such records transform into data surveillance as they are "repurposed, refined, and expanded for new problems, institutions, or applications" (Brayne 2018, p. 295).

Given this context, researchers are increasingly interested in how people respond to criminal legal system surveillance. Alice Goffman's (2014) ethnographic work describes strategic avoidance strategies for the men in her study who are subject to criminal legal system surveillance, developed further in Brayne's (2014) concept of systems avoidance, where people under police surveillance avoid institutions that collect formal records, including financial, medical, educational, and labor market institutions. Although some research has traced how criminal legal system surveillance has the potential to catalyze political engagement and protest (Rios 2011), more recent work has documented how people under surveillance strive for anonymity (Stuart 2016), tend to avoid institutional arrangements (Remster & Kramer 2018), disengage politically (Lerman & Weaver 2014), and experience legal cynicism (Kirk & Matsuda 2011) and legal estrangement (Bell 2017).

The duplication of criminal records across public- and private-sector contexts, and the resulting data error and uneven disclosure patterns, may exacerbate the effects of surveillance as it becomes increasingly difficult to manage the source. Qualitative research finds that confronting legal system surveillance and attempting to manage one's own criminal record data, such as when attempting to remedy an inaccurate criminal record or file for expungement, are disorienting and often infuriating processes that may lead to a sense of helplessness or an attempt to fly under the radar to evade a Google search that will uncover a criminal record (Lageson 2017).

Downloaded from www.annualreviews.org. Guest (guest) IP: 172.56.161.251 On: Sat, 24 Oct 2026 22:38:42

Criminal record surveillance may also block access to people's ability to assert their rights. In a 2012 concurring opinion for a police surveillance case, Justice Sonia Sotomayor argued that experiencing government surveillance "chills associational and expressive freedoms" and warned that "the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse" (*United States v. Jones* 2012). A RAND and National Institute of Justice Courts Advisory Panel analysis of courtroom innovation noted the risk of disincentivizing individuals to enter the court because of public disclosure requirements, bulk sales of court records, and challenges for expungement (RAND Corp. 2021). Legal and privacy scholars have long been concerned with the democratic and Constitutional consequences of surveillance, particularly when governmental records merge with or support private data collection and aggregation, putting individuals at increased risk for "dehumanization, powerlessness, and vulnerability" (Solove 2001, p. 1,140).

DIGITAL PUNISHMENT

Conceptually, this review has argued thus far that digital criminal records have transitioned from an administrative record of criminal legal system contact to new forms of digital stigma and digital surveillance. This section ultimately argues that the contemporary availability and uses of criminal records constitute digital punishment. Taking a sociology of punishment approach, I argue that digital records operate as an institutional form of punishment, or as "sociological effects and processes that are characteristic of penal systems" (Garland 2018). In this approach, criminal records might be viewed as an outgrowth, logic, or expression of legal punishments or as indicative of a broader culture of American punishment. Pragmatically, criminal record punishment has often been conceptualized through a collateral consequences lens, where social scientists measure stigma, discrimination, and burdens imposed by becoming the subject of a record. My conception of digital punishments builds on these theoretical and empirical interpretations of criminal records by pointing to specific dimensions of the digital context: The disordered nature of contemporary criminal records as complicating and expanding their effects, the commodification of records as contributing to what subjects perceive as eternal criminal punishment across public and private settings, and the effect of digital records as perpetuating criminal legal system biases and producing inequalities.

Disordered

A striking quality of contemporary criminal records is the fallibility of data in increasingly data-driven criminal justice operations (Logan & Ferguson 2016). Data quality issues have been central to debates over the spread and uses of criminal records and background checks (Logan & Ferguson 2016, McElhattan 2021, Urban Inst. 2017), thwarting reform efforts, like automatic sealing of records, due to dirty data that leaves people in "paper prisons" even in a digital world (Chien 2020). Missing case dispositions are a key data-integrity issue. Even in predigital contexts, experts warned that "the accuracy and completeness of criminal history information—the quality of data in those records—has emerged as perhaps the most significant information issue confronting the criminal justice community" (SEARCH Group 1985, p. 1). Two decades later, approximately half of the rap sheets maintained by the FBI failed to include final dispositions (US DOJ 2006). A recent report estimates an 80% error rate in criminal record databases (Rosenthal et al. 2015). A federal report showed that in 2012, seventeen states had more than 1.8 million unprocessed or partially processed disposition forms, with more than half of those states reporting that at least 30% of arrests in their records systems lacked any information on final disposition (US DOJ 2014).

Downloaded from www.annualreviews.org. Guest (guest) IP: 172.56.161.251 On: Sat, 24 Oct 2026 22:38:42

Downloaded from www.annualreviews.org. Guest (guest) IP: 172.56.161.251 On: Sat, 24 Oct 2026 22:38:42

Although American criminal records are generally thought of as public information, there is also significant unevenness in statutory guidance for releasing various types of criminal records (SEARCH Group 2005). Centralized rap sheets, for instance, are treated as a private record in approximately 50% of state jurisdictions (Lageson 2020, Sandoval & Lageson 2021), reflecting a 1989 Supreme Court ruling that a person enjoys a personal privacy interest in their rap sheets. Here, the Supreme Court considered how individuals would likely be "affected by the fact that in today's society the computer can accumulate and store information that would otherwise have surely been forgotten" (*Reporters Comm.* 1989, quoting *Department of the Air Force v. Rose* 1976) and coined the legal concept of "practical obscurity," the idea that although the individual components of the rap sheet include public information held by police and courts, the difficulty to access and compile this information creates a privacy protection (File 2017). Many states have followed this precedent, drawing distinct privacy boundaries around rap sheets but allowing the disclosure of arrest, court, and incarceration data through public records law. This means state policies often treat various types of criminal record data differently, depending on the originating source.

Because police, courts, jails, and prisons are in the public record, the criminal records they produce are the easiest and cheapest for the public to obtain. Yet these are the least reliable sources of criminal record data because they are not linked, harmonized, or updated to show the final case disposition. In sum, the contemporary criminal record originates from several sources, exists in multiple digital formats, and is disseminated differentially according to conflicting statutory guidance. Overall, there is a tendency for more extensive release of preconviction data at little or no cost to third parties. Governmental records that are affirmatively released from agencies are easily scraped, purchased, or duplicated by private entities and disclosed across a variety of web-based sources.

Given their local origins and differential patterns of disclosure, contemporary criminal records constitute an uncertain, ambiguous, and disordered type of punishment (Corda & Lageson 2020). Data are produced by thousands of different criminal justice agencies, often operating at the county or city level (Lageson et al. 2021). Records can lie dormant for years or decades and then reemerge on the Internet when a new source digitizes and releases archived criminal justice agency data (see, e.g., *Taha v. County of Bucks* 2017). Public, digital records may capture any point in a criminal case, documenting anything from a police stop that never led to criminal charges to information about a long-ago completed sentence (Corda 2016, Jacobs 2015). As records are downloaded, sold, and shared, they quickly become decontextualized and stale, often missing final disposition information (**Figure 2**) (Chien 2020) or failing to report an expungement or dismissal (Haber 2017).

With overlapping public- and private-sector uses, criminal record systems are markedly opaque and difficult to navigate or manage. The current landscape of criminal records has led to a "disorganized, consumer-based digital web of haphazard effects that do not neatly map onto information nor punishment functions" (Corda & Lageson 2020, p. 246). People who are the subjects of criminal records not only must contend with legally confusing, state-sanctioned labels (Myrick 2013) but often face incorrect information in their records (Lageson 2020, Logan & Ferguson 2016). The disordered nature of digital criminal records and poor data quality issues derive in large part from the institutional culture of criminal justice agencies, which are focused on local issues and distinct bureaucratic goals (Gray & Salole 2006), leading to fragmentations in procedures, implementation, and legal power. Within states or counties, each branch of law enforcement, courts, and correctional facilities develops distinct ideologies and practices around criminal record data collection and disclosure (RAND Corp. 2020). Criminal justice agencies must comply with a complex set of competing mandates, often with little legal guidance. Discretion thus becomes necessary for criminal justice workers to manage multifaceted directives.

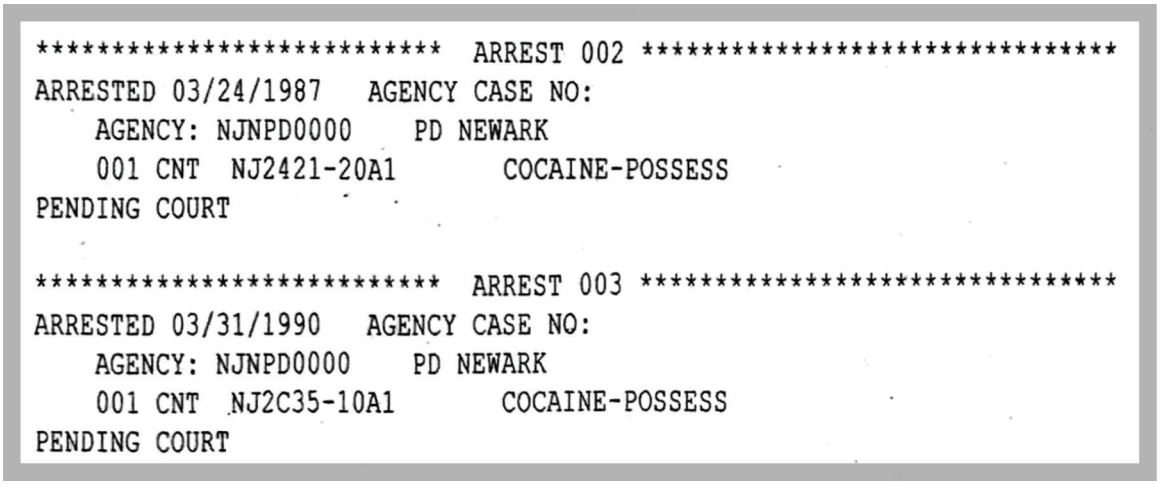

Figure 2

Missing criminal case dispositions from a research participant's New Jersey rap sheet (S.E. Lageson, unpublished data).

On the ground context matters for data quality. Criminal record keeping is deployed by administrative workers, increasingly tasked with managing voluminous data. However, decades of research into technological adaptation shows that, often, top-down policy is decoupled from frontline data handling and processing (Christin 2017), creating a situation in which the currents of two disparate groups—namely management and workers—run against one another in contested terrain (Edwards 1979), leading to foot-dragging and data obfuscation in criminal justice contexts (Brayne & Christin 2020). Although it might seem innovative to rely upon data-driven operations and algorithmic decision-making, researchers warn that these technological interventions "depend on the same good-old-fashioned factors that have helped and hindered reform for centuries: context, incentives, and details of implementation" (Stevenson 2018, p. 306).

Data-driven legal systems, which by design create more digital criminal records, depend heavily on employees tasked with learning and managing new technologies, changing their workflow patterns, and adhering to a new culture of intelligence-driven criminal justice administration. Criminal justice workers' viewpoints inadvertently shape data practices via their orientations toward governmental work, new technologies, and perspectives about how justice should be administered (Orlikowski 2000). The segmented nature of criminal justice operations exacerbates these decoupling processes, as external pressures and interagency conflict impact data collection and disclosure practices (Christin 2017), leading to confusion over how to interpret existing laws and policies (Lageson 2020). When facing uncertain mandates from policymakers to modernize criminal justice operations, organizations might imitate other agencies by adopting new technological tools but lack policies to dictate the on-the-ground changes in daily work routines necessary to achieve full implementation (DiMaggio & Powell 1983). Criminal justice workers are thus often left without the appropriate legal guidance to manage their decision-making about how to use new tools (Brayne & Christin 2020, Lageson 2020). Frontline workers must contend with institutionalized beliefs about the legality and rationality of new policies, such as sharing digital arrest information. In other words, the advent of digital technologies alone does not create digital punishment; rather, individual workers' compliance to new technological mandates also creates the reality of how justice administration operates (Edelman & Talesh 2011), leading to the data fragmentation and error that plagues contemporary record keeping and complicates our understanding of how exactly criminal record punishment is delivered and experienced.

Downloaded from www.annualreviews.org. Guest (guest) IP: 172.56.161.251 On: Sat, 24 Oct 2026 22:38:42

Commodified

Data released by police, courts, and correctional institutions have also become part of the Big Data economy. Private data brokers, "companies whose primary business is collecting personal information about consumers from a variety of sources and aggregating, analyzing, or sharing that information" (Fed. Trade Comm. 2014, p. 3), integrate criminal record data into other sources of personal data and public records (Crain 2018). This $200 billion industry profits through the commodification of data collected through broad commercial surveillance techniques (Crain 2018), incorporating data about criminal punishment into several corporate domains, including credit reporting, identity verification, fraud detection, and marketing (Fed. Trade Comm. 2014). In what is described by some scholars as a system of surveillance capitalism (Zuboff 2019), data brokers pay courts for bulk data sets that are repackaged with other sources of public and consumer data and then sold to background check services, market research companies, and even back to law enforcement (Etzioni 2016).

These trends are at least partly driven by consumer demand. Survey research shows approximately 38 million people (15% of Americans) search online for conviction records each year (Lageson et al. 2019). In response, personal data companies build marketing platforms on generous data assessments; for instance, Themis Data Solutions claims its repository holds 600 million unique criminal records, covering 90% of the US population (**https://www.themisds.com/Home/Products**), raising important questions about the economic value of such records that are disclosed as a public good and then commodified into valuable data.

The criminal record data economy and criminal background industry operate similarly to long-observed patterns of penal entrepreneurialism (Feeley 2002), wherein private actors work in concert with state actors to facilitate punishment, such as privatized prisons and probation operations (Feeley 2016). However, these paradigmatic forms of penal entrepreneurialism operated through contractual agreements between the state and the private entity. Today's criminal record industry increasingly operates outside the legal system in an opportunistic model that mines and repackages data produced by the state for commercial ends, pushing the limits of judicial oversight and governmental regulation (Corda & Lageson 2020). The private sector substantially extends the reach of the criminal legal system, or in Feeley's (2016, p. 1) terms, "expand[s] rather than contract[s] the reach of the state and the reach of the criminal sanction" as the information economy dramatically increases the quantity and quality of criminal records made available to consumers.

Alongside the widely accepted uses of criminal record data for employment background checks and tenant screening, cottage industries have developed on the Internet to monetize criminal record data through web advertising and search engine optimization or even to extort those who have been arrested. Mobile apps purport to update users about sex offenders and recent arrestees in their neighborhoods while simultaneously collecting and monetizing user data. Google search results for a person's name are accompanied by advertisements for background check and reputation management services. After a website posts a mugshot, the subject of the photo is charged staggering fees to have their photos removed, only to learn that the same photo was reposted by multiple other sites, a "twisted and expensive version of the childhood game 'whack-a-mole'" in which an arrestee is "desperately trying to permanently remove his mugshot from the web and inevitably failing" (Lee 2018, p. 560).

Technology and media companies also profit from widely available criminal record data, allowing local news sites a steady stream of arrests and mugshots that drive site traffic and increase advertising revenue (Hutchins 2018), reifying long-held critiques about racial disproportionality in reporting about crime (Beckett & Sasson 2003). However, there remains a strong consumer appetite for criminal justice news and infotainment, perhaps reflecting how the social aspects of

Downloaded from www.annualreviews.org. Guest (guest) IP: 172.56.161.251 On: Sat, 24 Oct 2026 22:38:42

public punishment have a moral function to solidify and express shared values through collective responses to crime (Katz 1987). Research has shown, for instance, how "the internet has become an expressive platform for people to use crime and punishment to expound on broader social issues and to anonymously—and sometimes viciously—identify, label, and digitally archive people as scapegoats for these problems" (Lageson & Maruna 2018, p. 115). Particularly in our punitive era, "the rituals of punishment are directed less at the individual offender than at the audience of impassioned onlookers whose cherished values and security had been momentarily undermined by the offender's actions" (Garland 1991, p. 123).

Biased

Digital criminal record data can create bias in two ways: First, the broad accessibility of online records can exacerbate criminal record–based discrimination, particularly against Black and Brown people and particularly for arrest and charging records that reflect discretion and bias by police and prosecutors. Second, criminal record data are routinely used for risk assessments, machine learning, and algorithmic predictions, but "using data from a racially biased criminal justice system can lead to unmeasurable biases in both risk scores and outcome measures" (Eckhouse et al. 2019, p. 185). The unquestioned use of criminal record data to justify surveillance, risk prediction, and sentences (Lynch & Bertenthal 2016) ignores the social foundation of how these records are created in the first place.

Empirical evidence of criminal record–based discrimination spans institutional and social sectors (Kirk & Wakefield 2018, Pager 2007, Uggen et al. 2014). The collateral consequences of a criminal record are widely documented, and the widespread disclosure of preconviction criminal record data may exacerbate these effects by implying criminality and legitimizing discriminatory practices regardless of legal guilt, raising due process and presumption of innocence concerns (Roberts 2019). Aided by the relative privacy protections of compiled criminal history reports (or rap sheets) compared to the wide availability of police and court-produced criminal record data (SEARCH Group 2005, Sandoval & Lageson 2021), the use of arrest records has become increasingly common and problematic in the Big Data age (Borchetta 2018). Rather than a conviction record that signals a constitutionally valid arrest or search, preconviction data reflect police and prosecutorial discretion, which disproportionately harms Black and Brown people in America.

Forty-six US states report some type of preconviction data on the Internet at no cost to users (Lageson et al. 2021). Preconviction data are disclosed primarily through police arrest records, pretrial jail detainment, and criminal court dockets. Arrest records, regardless of conviction, are increasingly used in a variety of domains, including "deportation, eviction, license suspension, custody disruption, and adverse employment actions" (Jain 2015, p. 809). Arrest records are also used within criminal justice system decision-making, "serving as a basis to justify future detentions by police and fueling a self-perpetuating cycle of criminal justice system contacts" (Logan & Ferguson 2016, p. 566) in the additive logic of increasingly managerial systems of surveillance and social control through the legal system (Kohler-Hausmann 2018). Criminal court data are routinely sold in bulk to private vendors and have been available on the Internet for at least two decades (SEARCH Group 2005), with a substantial number of states reporting charges that were dismissed or where the defendant was found not guilty. The high-volume and data-driven goals of American policing incentivize making more arrests, which create more police and court records that, once created, become public records that are increasingly impossible to seal or destroy.

The public disclosure of these front-end justice system processes may exacerbate the harms of the legal system on already disenfranchised communities (Western 2006). Studies show that even a police stop can lead to adverse outcomes (Sewell & Jefferson 2016), and the constant public

Downloaded from www.annualreviews.org. Guest (guest) IP: 172.56.161.251 On: Sat, 24 Oct 2026 22:38:42

reminder of arrest, detainment, or court experiences may create prolonged secondary effects. The technological aspects of digital punishment may also contribute to growing criminal legal system inequalities, as those with legal, financial, or technological resources may be more likely to directly address and remedy their online criminal records through obtaining better legal outcomes (such as a dismissal or deferred adjudication), hiring an attorney to file for a criminal record expungement, or paying an Internet reputation management service to pressure websites to take down records (Lageson 2020). Studies confirm the disparate impact of Big Data technologies on already-marginalized populations (Barocas & Selbst 2016) and class differentials in privacy intrusions (Gilman 2012). This aspect is further exacerbated for marginalized groups and people of color, who are already under intense regimes of surveillance and monitoring through the administration of public benefits, subsidized housing, medical care, and legal aid (Eubanks 2018). Put differently, digital punishment unequally stigmatizes already marginalized and socially ostracized groups, who are simultaneously less able to address, remedy, or overcome a digital criminal record.

POLICY IMPLICATIONS

The legal and social contexts that have allowed for the broad dissemination and commodification of criminal record data also pose obstacles for increasingly popular criminal legal system reforms. Digital criminal record keeping, the disclosure and aggregation of criminal record data, and the consequences for stigma and punishment have also complicated policy debates over government transparency, the role of Big Tech in criminal legal operations, and the efficacy of criminal record reforms, such as record sealing, expungement, Ban the Box, and Clean Slate policies. This section briefly describes these central policy debates and offers guidance for researchers seeking to inform these questions.

Government Transparency

As described above, legislative guidance and public policy arguments for the release of criminal record data are often rooted in governmental transparency, public records accessibility, and the Freedom of Information Act (FOIA). However, the original intent of transparency laws to aid in governmental watchdogging bears little similarity to how transparency operates today. A 2017 analysis of 229,000 FOIA requests to eighty-five government agencies, for instance, found that only 7.6% of requests were made by journalists and the news media, whereas 39% were made by commercial businesses for largely profit-seeking, rather than watchdogging, efforts (Galka 2017). Private-sector uses of public records lead to a "reverse sunshine effect," where the push for open access to public records has become a "double-edged sword. . .public records primarily contain information on private individuals rather than information on government officials" (Brobst 2015). The inclusion of personally identifiable information (see **Figure 3**) adds new, and potentially problematic, dimensions to the long-standing arguments for access to criminal record data. In the past, the "right to know" about a person's criminal legal entanglements typically would include the type and date of offense but is now expanded to include their height, weight, birth date, physical characteristics, and home address.

The focus on sharing and monetizing information about arrestees and defendants rather than governmental actors "runs directly counter to the spirit of freedom of information laws, which were designed to empower individuals to monitor their government, not vice versa" (Solove 2004, p. 153). Rather than data that shed light on the way the government carries out its functions, personal information contained in public records "reveals more about the people who are subjects of the government's regulatory machinery" (Solove 2004, p. 150). The disclosures of personally identifiable data about arrestees, detainees, and defendants also stand in contrast to a relative lack

Downloaded from www.annualreviews.org. Guest (guest) IP: 172.56.161.251 On: Sat, 24 Oct 2026 22:38:42

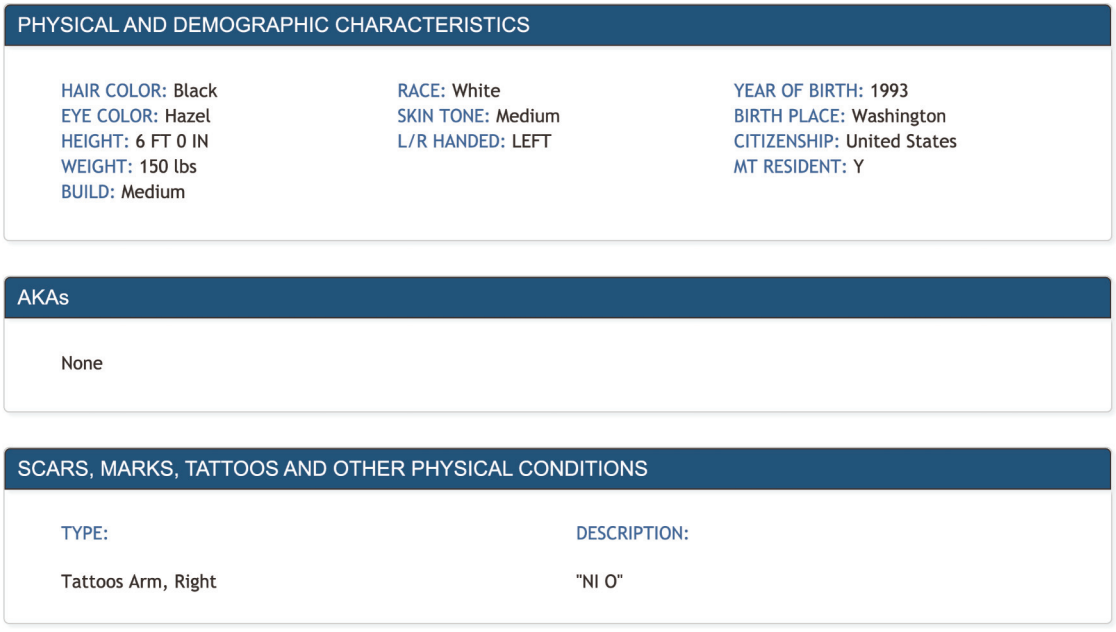

Figure 3

Personal identifiers, such as skin tone, hair color, and tattoos, as posted on the internet in the Montana prison inmate online database.

of transparency and aggregate data about many components of the legal system, including police misconduct (Conti-Cook 2017), prosecutorial discretion (Sklansky 2018), and plea bargains (Johnson 2020). A lack of integrated systems-level criminal justice data also has consequences for empirical research: Kirk & Wakefield (2018, p. 177) note that serious limitations in collateral consequences research "result from a lack of appropriate and detailed data on criminal justice processing." Encouraging standardized, robust data collection that includes detailed information about criminal justice actors and requires research ethics–based privacy regulations would improve criminological understandings of how the legal system works across jurisdictions and over time.

The Role of Big Tech in Legal Systems

The private sector is an integral part of the digital criminal records infrastructure. Private technology companies develop, market, and sell tools to criminal justice agencies to aid data collection and analytic efforts. Private companies then purchase, scrape, or mine these same criminal justice system data for profit-seeking endeavors. Criminal justice agencies also benefit from private-sector data collection efforts, where consumer, marketing, and financial records aggregated for noncriminal justice purposes are used for intelligence and crime prediction (Brayne 2017). Police departments use facial-recognition software developed through social media image scraping (Klosowski 2020) and can obtain surveillance footage from Amazon Ring video doorbells voluntarily installed by civilians; by early 2021, all but two US states had a police or fire department that has entered into Amazon's Ring Network, creating more than 2,000 Amazon–criminal justice agency partnerships (Lyons 2021).

Yet the private sector is also making claim to assisting and even leading criminal justice reform efforts through technological innovation. The political strategist David Plouffe wrote in 2019,

Downloaded from www.annualreviews.org. Guest (guest) IP: 172.56.161.251 On: Sat, 24 Oct 2026 22:38:42

after joining the Facebook founder's Chan Zuckerberg Initiative (CZI), that technology should be "appropriately harnessed to help key actors in the justice system make evidence-based decisions, and move toward something that's fairer, more equitable, more transparent, and actually safety-oriented" (Plouffe 2019). CZI and Code for America are active in the Clean Slate Initiative, a "bipartisan policy model that uses technology to automatically clear criminal records if a person stays crime-free" (**https://cleanslateinitiative.org/**). In 2017, Google appropriated $7.5 million to criminal justice reform (Google 2017). However, Google and Facebook remain key conduits for how the public learns about and accesses criminal record information (Lageson 2020). In a permissive American legal environment that allows for the legal dissemination of criminal record data, company policy (rather than governmental regulation) may be the most direct path to easing the burden of criminal records by allowing people to request that content about their criminal records be taken down after a requisite time period or postexpungement.

The influence of technology companies has long been part of modern criminal justice operations, but these interdependencies have accelerated in our data-driven world, creating new research questions and new sources of data. For instance, Harris et al. (2019) recently developed the concept of cost points to describe how individuals who make contact with public systems of justice may be charged fees by private entities for court-imposed programming, management, or surveillance, analyzing the extent to which private companies generate profit through criminal justice partnerships. Additional criminological research into the development, efficacy, and consequences of these partnerships is sorely needed (particularly for those that introduce new technological tools into the legal system) if we hope to capture a more accurate portrait of contemporary criminal justice operations.

Clean Slate Policies

A final policy-relevant dimension to digital criminal records involves the sealing or expunging of criminal records. Across the United States, advocates and policymakers are working in earnest to pass criminal record expungement legislation: In 2018 alone, 20 states enacted or expanded expungement legislation (Collat. Conseq. Resour. Cent. 2019). Sweeping reform continued in 2019 and 2020 as states began to adopt automated and algorithmic means of record sealing, supported by nationwide efforts like the Clean Slate Initiative. By 2020, more than two-thirds of US states have some sort of law that allows for a criminal record to be concealed from public view through record sealing or expungement.

Criminal record sealing first gained attention in the 1940s and 1950s, based on the notion that criminal records' lasting nature could deprive people of fundamental civil, political, and economic rights (Love 2002). But by the 1970s, criminal justice experts began to warn that efforts to expunge records constituted a Big Lie (Kogan & Loughery 1970). These critics claimed the process would be unworkable and unenforceable, particularly because criminal records are maintained by distinct agencies, and thus "encourages harmful speculation and distorts the record with half-truths" (Kogan & Loughery 1970, p. 385). This, argued the authors, could work to the criminal record subjects' disadvantage if employers or the broader public fill in the blanks with stereotypical or sensationalist editorializing. The most enduring consequence, however, was that expungement "help[s] society evade its obligation to change its views toward former offenders. Instead of accepting ex-law breakers and giving them a fair chance, the community requires them to lie, and the community lies to itself when it conceals their records in order to make them employable. This violates every principle of honest rehabilitation work" (Kogan & Loughery 1970, p. 378).

The difficulties in obtaining a truly clean slate in an American digital criminal records context are clear: Expungement can address only the governmental version of a record, leaving intact

Downloaded from www.annualreviews.org. Guest (guest) IP: 172.56.161.251 On: Sat, 24 Oct 2026 22:38:42

Google search results and criminal record data already aggregated into private databases (Lageson 2020). Other criminal justice reform efforts that rely on privacy or secrecy have seen mixed results. For instance, Ban the Box policies (mandating the removal of criminal record questions from job applications) showed little to no impact on private-sector employment of people with records and instead showed evidence of statistical discrimination by harming the employment prospects of African American men (Raphael 2021). An empirical study of expungement outcomes in Michigan found both a positive effect for employment and low recidivism among those who received an expungement, but with the caveat that only 6.5% of eligible people obtained an expungement (Prescott & Starr 2020), known as the second-chance gap (Chien 2020). Public opinion for expungement is a bit mixed. One recent public opinion survey found that although nearly 55% of respondents were opposed to expungement, support increases based on time since offense and type of offense (specifically, the majority of respondents supported expungement of convictions from more than seven years prior and for nonviolent offenses) (Burton et al. 2021). However, the debates around criminal record reform are a window into criminological debates over punishment, risk, rehabilitation, and forgiveness. This review concludes with a reflection on those themes.

IS DIGITAL PRIVACY LOSS A COLLATERAL CONSEQUENCE?

In many ways, digital criminal records reflect broader social and political choices about criminal punishment and the legal system. Just as our contemporary system is marked by mass incarceration and mass supervision, so too are the Big Data that catalog the experience of millions who are processed through criminal legal channels. Although there may be methodological and public safety– and justice-related benefits to collecting, sharing, and analyzing mass troves of criminal record data, the notion of eternal digital punishment has complicated these benefits. Criminal records now pose questions that intersect with broader social debates over digital privacy rights and the right to be forgotten.

In terms of how digital records fit into the culture of American punishment, scholars might view the trends described here as an expansion of the culture of control (Garland 2001) into virtual spaces, fueled by new levels of fear and insecurity. Digital stigma might represent a new "technology of exile" (Simon 2007, p. 172), in which the cultural project of socially isolating potentially threatening persons is sustained largely by private parties, such as the website operators who post mugshots and the neighbors who avoid the community member who appears on the website. Yet there are important caveats to consider. Criminal record data are part of the broader data ecosystem of the criminal legal system, and decades of research have utilized these data to identify and critique the foundational racial injustice of the system (Johnson & Rostain 2020). After George Floyd was murdered in 2020, public demand for transparency in criminal justice has created pathways for new legislation and increased watchdogging of police, prosecutors, and judges. Scholars note the possibilities for Big Data to become "bright data" (Ferguson 2017) or "data as spotlight" (Johnson & Rostain 2020) that illuminate problematic and harmful patterns in policing and courts.

Judicial views about the value of transparency against the loss of personal privacy have shifted over time. In *Paul v. Davis* (1976), the Supreme Court declined to extend a privacy right to a person whose mugshot was distributed by local police after he was arrested for shoplifting. The court held that stigmatization through publicizing an official act of government (here, an arrest) did not deprive the petitioner of privacy nor liberty rights under the Due Process Clause of the Fourteenth Amendment. The dissent in the 5–3 decision, however, issued a warning that the decision meant police could "on their own initiative and without trial constitutionally condemn innocent individuals as criminals and thereby brand them with one of the most stigmatizing and debilitating labels in our society" (*Paul v. Davis* 1976).

Downloaded from www.annualreviews.org. Guest (guest) IP: 172.56.161.251 On: Sat, 24 Oct 2026 22:38:42

In 1996, the Sixth Circuit heard a case between a newspaper and the Department of Justice over the release of mugshots. The Appellate Court ruled for the newspaper, holding that mugshots of federal arrestees did not violate their privacy rights (*Detroit Free Press Inc. v. US Department of Justice* 1996). Two decades later, that case was overturned in the same court (*Detroit Free Press Inc. v. US Department of Justice* 2016), this time finding that individuals do have a privacy interest in their mugshot, i.e., that a "disclosed booking photo casts a long, damaging shadow over the depicted individual. . . . Today, an idle internet search reveals the same booking photo that once would have required a trip to the local library's microfiche collection. In fact, mug-shot websites collect and display booking photos from decades-old arrests." In a concurring opinion, Chief Judge Cole (*Detroit Free Press Inc. v. US Department of Justice* 2016) considered that:

> Twenty years ago, we thought that the disclosure of booking photographs, in ongoing criminal proceedings, would do no harm. But time has taught us otherwise. The internet and social media have worked unpredictable changes in the way photographs are stored and shared. Photographs no longer have a shelf life, and they can be instantaneously disseminated for malevolent purposes. Mugshots now present an acute problem in the digital age: these images preserve the indignity of a deprivation of liberty, often at the (literal) expense of the most vulnerable among us.

Although this case was brought by media to gain access to criminal justice records, newspapers have also begun to backtrack on previously staunch views about the right to access and publish criminal record information. In the last year, the *Houston Chronicle*, Cleveland.com, and Gannett Media (which owns dozens of newspapers) removed mugshot galleries from their online content. In June 2021, the AP announced it would no longer report the names of people accused of minor crimes due to the harm to their digital reputation. Recognizing their role as digital content creators, some police departments have simply ended the practice of posting mugshots on their Facebook sites, acknowledging that although it is legal, it is no longer necessary.

The shifting arguments by courts, media, and transparency advocates may signal broader tensions about whether privacy loss might be considered an emerging collateral consequence of justice system contact. Social scientists have wrestled with how to understand privacy in various social contexts and how to incorporate social structure and inequality into privacy rights (Baghai 2012). A social scientific view squarely frames privacy as a "resource that is unequally distributed in society," which in turn means that the "production and management of privacy may create inequality among social actors" (Anthony et al. 2017, p. 259). Emerging sociological and criminological conceptions of privacy, then, should ask questions not only about individual autonomy and control over one's personal information but also about access and equity to privacy rights at all, particularly given the inequalities produced through the criminal legal system.

The contemporary functions and harms of digital criminal records provide evidence for a broader, normative reconceptualization of how criminal records ought to be developed, shared, and used across social contexts, with specific attention paid to digital privacy harms as a collateral consequence. Relatedly, criminologists might consider the role of forgetting in the process of rehabilitation and desistance. William James wrote in 1892 that in the "practical use of our intellect, forgetting is as important a function as remembering" (James 1892, p. 300). Forgetting, wrote Meg Leta Jones (2018, p. 300) more than a century later, is "intended to free individuals from the weight of their digital baggage. It is a larger cultural willingness to allow individuals to move beyond their personal pasts, a societal capacity to offer forgiveness, provide second chances, and recognize the value of reinvention." In Europe, the "Right to Be Forgotten" is the first international law to directly address the power of technology and data companies to write our digital biographies without our control or consent by allowing users to have content removed from Internet search results, including criminal records. For effective rehabilitation and desistance, our

Downloaded from www.annualreviews.org. Guest (guest) IP: 172.56.161.251 On: Sat, 24 Oct 2026 22:38:42

legal systems may need to consider embracing digital privacy and controlling the flow of criminal record information by regulating these records by the same standards afforded to credit reports, medical histories, and student data.

Although privacy has been somewhat neglected by criminology, our Big Data world demands new attention to how technology has reshaped punishment, collateral consequences, and legal consciousness. In 1970, former US Attorney General Ramsey Clark wrote about the need for privacy in the administration of justice. Invasions of privacy, he argued, "demean the individual. . . . When a government degrades its citizens, or permits them to degrade each other, however beneficent the specific purpose, it limits opportunities for individual fulfillment and national accomplishment." In the end, he argues, the price will be "dear indeed. The practice is incompatible with a free society" (Clark 1970, p. 287). As we reckon with facial-recognition technologies, license plate readers, real-time GPS tracking, and predictive policing, questions about the role of privacy within criminological understandings of the world will only grow more urgent.

DISCLOSURE STATEMENT

The author is not aware of any affiliations, memberships, funding, or financial holdings that might be perceived as affecting the objectivity of this review.

LITERATURE CITED

Anthony D, Campos-Castillo C, Horne C. 2017. Toward a sociology of privacy. *Annu. Rev. Sociol.* 43:249–69

Baghai K. 2012. Privacy as a human right: a sociological theory. *Sociology* 46(5):951–65

Barocas S, Selbst AD. 2016. Big data's disparate impact. *Calif. Law Rev.* 104:671–732

Beckett K, Sasson T. 2003. *The Politics of Injustice: Crime and Punishment in America*. Thousand Oaks, CA: SAGE

Bell MC. 2017. Police reform and the dismantling of legal estrangement. *Yale Law J.* 126:2054–150

Benjamin R. 2019. *Race After Technology: Abolitionist Tools for the New Jim Code*. Cambridge, UK: Polity Press

Blumstein A, Nakamura K. 2009. Redemption in the presence of widespread criminal background checks. *Criminology* 47(2):327–59

Borchetta JR. 2018. Curbing collateral punishment in the big data age: how lawyers and advocates can use criminal record sealing statutes to protect privacy and the presumption of innocence. *Boston Univ. Law Rev.* 98:915–51

Bowker GC, Star SL. 2000. *Sorting Things Out: Classification and its Consequences*. Cambridge, MA: MIT Press

Brackett C. 2020. *The rise and rise of the criminal record: power, order, and safety in the United States, 1848–1960*. PhD Diss., Univ. Mass., Boston, MA

Brame R, Bushway SD, Paternoster R, Turner MG. 2014. Demographic patterns of cumulative arrest prevalence by ages 18 and 23. *Crime Delinquency* 60(3):471–86

Brame R, Turner MG, Paternoster R, Bushway SD. 2012. Cumulative prevalence of arrest from ages 8 to 23 in a national sample. *Pediatrics* 129(1):21–27

Brandeis L. 1913. What publicity can do. *Harper's Weekly*. Dec. 20

Brayne S. 2014. Surveillance and system avoidance: criminal justice contact and institutional attachment. *Am. Sociol. Rev.* 79(3):367–91

Brayne S. 2017. Big data surveillance: the case of policing. *Am. Sociol. Rev.* 82(5):977–1008

Brayne S. 2018. The criminal law and law enforcement implications of big data. *Annu. Rev. Law Soc. Sci.* 14:293–308

Brayne S, Christin A. 2020. Technologies of crime prediction: the reception of algorithms in policing and criminal courts. *Soc. Probl.* 68(3):608–24

Brobst JA. 2015. Reverse sunshine in the digital wild frontier: protecting individual privacy against public records requests for government databases. *North. Ky. Law Rev.* 42:191–286

Burton AL, Cullen FT, Pickett JT, Burton VS Jr., Thielo AJ. 2021. Beyond the eternal criminal record: public support for expungement. *Criminol. Public Policy* 20(1):123–51

Downloaded from www.annualreviews.org. Guest (guest) IP: 172.56.161.251 On: Sat, 24 Oct 2026 22:38:42

Downloaded from www.annualreviews.org. Guest (guest) IP: 172.56.161.251 On: Sat, 24 Oct 2026 22:38:42

Bushway SD, Stoll MA, Weiman D, eds. 2007. *Barriers to Reentry?: The Labor Market for Released Prisoners in Post-Industrial America*. New York: Russell Sage Found.

Chien C. 2020. America's paper prisons: the second chance gap. *Mich. Law Rev.* 119(3):519–612

Chiricos T, Barrick K, Bales W, Bontrager S. 2007. The labeling of convicted felons and its consequences for recidivism. *Criminology* 45(3):547–81

Christin A. 2017. Algorithms in practice: comparing web journalism and criminal justice. *Big Data Soc.* 2017:1–14

Clair M. 2021. Criminalized subjectivity: Du Boisian sociology and visions for legal change. *Du Bois Rev. Soc. Sci. Res. Race*. In press

Clark R. 1970. *Crime in America: Observations on its Nature, Causes, Prevention and Control*. New York: Simon & Schuster

Collat. Conseq. Resour. Cent. 2019. *Updated report on 2018 fair chance and expungement reforms*. Rep., Collat. Conseq. Resour. Cent., Washington, DC. **http://ccresourcecenter.org/2019/03/28/updated-report-on-2018-fair-chance-and-expungement-reforms/**

Conley A, Datta A, Nissenbaum H, Sharma D. 2011. Sustaining privacy and open justice in the transition to online court records: a multidisciplinary inquiry. *Md. Law Rev.* 71:772–847

Conti-Cook CH. 2017. Open data policing. *Georget. Law J.* 106:1–23

Corda A. 2016. More justice and less harm: reinventing access to criminal history records. *Howard Law J.* 60:1–60

Corda A, Lageson SE. 2020. Disordered punishment: workaround technologies of criminal records disclosure and the rise of a new penal entrepreneurialism. *Br. J. Criminol.* 60(2):245–64

Crain M. 2018. The limits of transparency: data brokers and commodification. *New Media Soc.* 20(1):88–104

Department of the Air Force v. Rose, 425 U.S. 352 (1976)

Detroit Free Press Inc. v. US Department of Justice, 73 F.3d 93 (6th Cir. 1996)

Detroit Free Press Inc. v. US Department of Justice, 829 F.3d 478 (6th Cir. 2016)

DiMaggio PJ, Powell WW. 1983. The iron cage revisited: institutional isomorphism and collective rationality in organizational fields. *Am. Sociol. Rev.* 48(2):147–60

Eckhouse L, Lum K, Conti-Cook C, Ciccolini J. 2019. Layers of bias: a unified approach for understanding problems with risk assessment. *Crim. Justice Behav.* 46(2):185–209

Edelman LB, Talesh SA. 2011. To comply or not to comply—that isn't the question: how organizations construct the meaning of compliance. In *Explaining Compliance: Business Responses to Regulation*, ed. C Parker, VL Nielsen, pp. 103–22. Northamption, MA: Edward Elgar

Edwards R. 1979. *Contested Terrain: The Transformation of the Workplace in the Twentieth Century*. New York: Basic Books

Etzioni A. 2016. Reining in private agents. *Minn. Law Rev.* 101:279–331

Eubanks V. 2018. *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. New York: St. Martin's Press

Fed. Trade Comm. 2014. *Data brokers: a call for transparency and accountability*. Rep., Fed. Trade Comm., Washington, DC. **https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf**

Feeley MM. 2002. Entrepreneurs of punishment: the legacy of privatization. *Punishm. Soc.* 4:321–44

Feeley MM. 2016. Entrepreneurs of punishment: how private contractors made and are remaking the modern criminal justice system—an account of convict transportation and electronic monitoring. *Criminol. Crim. Justice Law Soc.* 17(3):1–30

Ferguson AG. 2017. *The Rise of Big Data Policing*. New York: NYU Press

File PC. 2017. A history of practical obscurity: clarifying and contemplating the twentieth century roots of a digital age concept of privacy. *Univ. Balt. J. Media Law Ethics* 6:4–21

Foucault M. 1977. *Discipline and Punish: The Birth of the Prison*. New York: Pantheon

Galka M. 2017. Who uses FOIA? An analysis of 229,000 requests to 85 government agencies. *FOIA Mapper*. **https://foiamapper.com/who-uses-foia/**

Garland D. 1991. Sociological perspectives on punishment. *Crime Justice* 14:115–65

Garland D. 1997. Governmentality and the problem of crime: Foucault, criminology, sociology. *Theor. Criminol.* 1(2):173–214
Garland D. 2001. *The Culture of Control: Crime and Social Order in Contemporary Society*. Chicago: Univ. Chicago Press
Garland D. 2018. Theoretical advances and problems in the sociology of punishment. *Punishm. Soc.* 20(1):8–33
Gilman ME. 2012. The class differential in privacy law. *Brooklyn Law Rev.* 77(4):1389–445
Giordano PC, Cernkovich SA, Rudolph JL. 2002. Gender, crime, and desistance: toward a theory of cognitive transformation. *Am. J. Sociol.* 107(4):990–1064
Goffman A. 2014. *On the Run: Fugitive Life in an American city*. Chicago: Univ. Chicago Press
Goffman E. 1963. *Stigma: Notes on the Management of Spoiled Identity*. New York: Simon Schuster
Google. 2017. *Two years of Google.org grants for racial justice*. Press Release, Novemb. 21. **https://blog.google/outreach-initiatives/google-org/two-years-supporting-racial-justice/**
Gray GC, Salole AT. 2006. The local culture of punishment: an ethnography of criminal justice worker discourse. *Br. J. Criminol.* 46(4):661–79
Gurusami S. 2019. The carceral web we weave: carceral citizens' experiences of digital punishment and solidarity. *Punishm. Soc.* 21(4):435–53
Haber E. 2017. Digital expungement. *Md. Law Rev.* 77:337–84
Haggerty KD, Ericson RV. 2006. *The New Politics of Surveillance and Visibility*. Toronto: Univ. Tor. Press
Hannah-Moffat K. 2019. Algorithmic risk governance: big data analytics, race and information activism in criminal justice debates. *Theor. Criminol.* 23(4):453–70
Harris A, Smith T, Obara E. 2019. Justice "cost points" examination of privatization within public systems of justice. *Criminol. Public Policy* 18(2):343–59
Hu M. 2015. Big data blacklisting. *Fla. Law Rev.* 67:1735–809
Hutchins C. 2018. Mugshot galleries might be a web-traffic magnet. Does that justify publishing them? *Columbia Journalism Review*, Oct. 24. **https://www.cjr.org/united_states_project/mugshots-ethics.php**
Jacobs JB. 2015. *The Eternal Criminal Record*. Cambridge, MA: Harv. Univ. Press
Jain E. 2015. Arrests as regulation. *Stanf. Law Rev.* 67:809–67
James W. 1892. *Textbook of Psychology*. London: Macmillan & Co
Johnson RA, Rostain T. 2020. Tool for surveillance or spotlight on inequality? Big data and the law. *Annu. Rev. Law Soc. Sci.* 16:453–72
Johnson T. 2020. Crisis and coercive pleas. *J. Crim. Law Criminol.* 110:1–22
Jones ML. 2018. *Ctrl + Z: The Right to be Forgotten*. New York: NYU Press
Kaspero E, Canhasi D. 2018. *Criminal record privacy & the structural risks inherent within commercial storehouses in the consumer data industry*. SSRN Work. Pap. 3130418
Katz J. 1987. What makes crime news? *Media Cult. Soc.* 9(1):47–75
Kirk DS, Matsuda M. 2011. Legal cynicism, collective efficacy, and the ecology of arrest. *Criminology* 49(2):443–72
Kirk DS, Wakefield S. 2018. Collateral consequences of punishment: a critical review and path forward. *Annu. Rev. Criminol.* 1:171–94
Kogan B, Loughery DL Jr. 1970. Sealing and expungement of criminal records: the big lie. *J. Crim. Law Criminol. Police Sci.* 61(3):378–92
Kohler-Hausmann I. 2018. *Misdemeanorland: Criminal Courts and Social Control in an Age of Broken Windows Policing*. Princeton, NJ: Princeton Univ. Press
Klosowski T. 2020. Facial recognition is everywhere. Here's what we can do about it. *New York Times*, July 15. **https://www.nytimes.com/wirecutter/blog/how-facial-recognition-works/**
Lageson SE. 2017. Crime data, the internet, and free speech: an evolving legal consciousness. *Law Soc. Rev.* 51(1):8–41
Lageson SE. 2020. *Digital Punishment: Privacy, Stigma and the Harms of Data-Driven Criminal Justice*. New York: Oxford Univ. Press
Lageson SE, Denver M, Pickett JT. 2019. Privatizing criminal stigma: experience, intergroup contact, and public views about publicizing arrest records. *Punishm. Soc.* 21(3):315–41

Downloaded from www.annualreviews.org. Guest (guest) IP: 172.56.161.251 On: Sat, 24 Oct 2026 22:38:42

Lageson SE, Maruna S. 2018. Digital degradation: stigma management in the internet age. *Punishm. Soc.* 20(1):113–33

Lageson SE, Webster E, Sandoval JR. 2021. Digitizing and disclosing personal data: the proliferation of state criminal records on the internet. *Law Soc. Inq.* 46(3):635–65

Laub JH, Sampson RJ. 1993. Turning points in the life course: why change matters to the study of crime. *Criminology* 31(3):301–25

Lee EK. 2018. Monetizing shame: mugshots, privacy, and the right to access. *Rutgers Univ. Law Rev.* 70(3):557–645

Lerman AE, Weaver V. 2014. Staying out of sight? Concentrated policing and local political action. *Ann. Am. Acad. Political Soc. Sci.* 651(1):202–19

Link BG, Phelan JC. 2001. Conceptualizing stigma. *Annu. Rev. Sociol.* 27:363–85

Logan WA. 2009. *Knowledge as Power*: *Criminal Registration and Community Notification Laws in America*. Stanford, CA: Stanf. Univ. Press

Logan WA. 2018. Policing police access to criminal justice data. *Iowa Law Rev.* 104:619–78

Logan WA, Ferguson AG. 2016. Policing criminal justice data. *Minn. Law Rev.* 101:541–616

Logan WA, Prescott JJ. 2021. *Sex Offender Registration and Community Notification Laws*: *An Empirical Evaluation*. Cambridge, UK: Cambridge Univ. Press

Love MC. 2002. Starting over with a clean slate: in praise of a forgotten section of the model penal code. *Fordham Urban Law J.* 30:101–36

Luca DL. 2018. *The digital scarlet letter*: *the effect of online criminal records on crime*. Work. Pap. 1118, Univ. Mo., Columbia, MO

Lynch M, Bertenthal A. 2016. The calculus of the record: criminal history in the making of US federal sentencing guidelines. *Theor. Criminol.* 20(2):145–64

Lyon D. 2007. *Surveillance Studies*: *An Overview*. Cambridge, UK: Polity Press

Lyons L. 2021. Amazon's Ring now reportedly partners with more than 2,000 US police and fire departments. *The Verge*, January 31. **https://www.theverge.com/2021/1/31/22258856/amazon-ring-partners-police-fire-security-privacy-cameras**

Maruna S. 2001. *Making Good*: *How Ex-Convicts Reform and Rebuild Their Lives*. Washington, DC: Am. Psychol. Assoc.

Matza D. 1969. *Becoming Deviant*. New Brunswick, NJ: Transaction Publ.

McElhattan D. 2018. "$40 to make sure": background check laws and the endogenous construction of criminal risk. In *After Imprisonment*, ed. A Sarat, pp. 99–121. Bingley, UK: Emerald Publ.

McElhattan D. 2021. Punitive ambiguity: state-level criminal record data quality in the era of widespread background screening. *Punishm. Soc.* **https://doi.org/10.1177/1462474521989502**

Myrick A. 2013. Facing your criminal record: expungement and the collateral problem of wrongfully represented self. *Law Soc. Rev.* 47(1):73–104

Nixon v. Warner Communications, Inc., 435 U.S. 589 (1978)

Orlikowski WJ. 2000. Using technology and constituting structures: a practice lens for studying technology in organizations. *Organ. Sci.* 11(4):404–28

Pager D. 2007. *Marked*: *Race*, *Crime*, *and Finding Work in an Era of Mass Incarceration*. Chicago: Univ. Chicago Press

Paul v. Davis, 424 U.S. 693 (1976)

Phelps MS. 2020. Mass probation from micro to macro: tracing the expansion and consequences of community supervision. *Annu. Rev. Criminol.* 3:261–79

Plouffe D. 2019. How technology can build a more equitable justice system. *Fast Company*, March 6. **https://www.fastcompany.com/90315651/how-technology-can-help-build-a-more-equitable-justice-system**

Prescott JJ, Starr SB. 2020. Expungement of criminal convictions: an empirical study. *Harv. Law Rev.* 133:2460–555

RAND Corp. 2020. *Comparison of criminal history information systems in the United States and other countries*. Rep., RAND Corp., Santa Monica, CA. **https://www.rand.org/randeurope/research/projects/criminal-history-information-systems.html**

Downloaded from www.annualreviews.org. Guest (guest) IP: 172.56.161.251 On: Sat, 24 Oct 2026 22:38:42

RAND Corp. 2021. Tool for ranking courts innovations needs. Rep., RAND Corp., Santa Monica, CA. **https://www.rand.org/well-being/justice-policy/projects/priority-criminal-justice-needs/courts/interactive-tool.html**

Raphael S. 2021. The intended and unintended consequences of ban the box. *Annu. Rev. Criminol.* 4:191–207

Rempel W. 1986. Dossier society: computers: Is privacy the loser? *Los Angeles Times*. July 29. **https://www.latimes.com/archives/la-xpm-1986-07-29-mn-19580-story.html**

Remster B, Kramer R. 2018. Race, space, and surveillance: understanding the relationship between criminal justice contact and institutional involvement. *Socius Sociol. Res. Dyn. World* 4:1–16

Reporters Comm., 489 U.S 769 (1989)

Republic of the Philippines v. Westinghouse Electric Corp., 949 F.2d 653 (3d Cir. 1991)

Res. Mark. 2018. *Employment screening service market to 2025—global analysis & forecasts by services* (*background screening*, *verification*, *medical testing & electronic auditing*); *& application* (*financial services*, *government agencies*, *transportation*, *industrial*). Rep., Res. Mark., Dublin, Irel. **https://www.researchandmarkets.com/research/nf5vfq/5_46_billion?w=4**

Restivo E, Lanier MM. 2015. Measuring the contextual effects and mitigating factors of labeling theory. *Justice Q.* 32(1):116–41

Rios VM. 2011. *Punished*: *Policing the Lives of Black and Latino Boys*. New York: NYU Press

Roberts A. 2019. Arrests as guilt. *Ala. Law Rev.* 70:987–1030

Rosenthal A, NaPier E, Warth P, Weissman M. 2015. *Boxed out*: *criminal history screening and college application attrition*. Rep., Cent. Community Altern., Brooklyn, NY. **https://www.communityalternatives.org/wp-content/uploads/2019/11/boxed-out.pdf**

Sampson RJ, Laub JH. 2003. Life-course desisters? Trajectories of crime among delinquent boys followed to age 70. *Criminology* 41(3):555–92

Sandoval JR, Lageson SE. 2021. *Patchwork disclosure*: *divergent public access and personal privacy across criminal record disclosure policy in the United States*. Work. Pap., Univ. Calif., Irvine

SEARCH Group. 1985. *Data quality of criminal history records*. Bur. Justice Stat. Rep., US Dep. Justice, Washington, DC. **https://bjs.ojp.gov/content/pub/pdf/dqchr.pdf**

SEARCH Group. 2005. *Report of the National Task Force on Privacy*, *Technology and Criminal Justice Information*. Rep. NCJ 187669, US Dep. Justice, Washington, DC. **https://bjs.ojp.gov/content/pub/pdf/rntfptcj.pdf**

Sentencing Proj. 2014. *Americans with criminal records*. Rep., Sentencing Proj., Washington, DC. **https://www.sentencingproject.org/wp-content/uploads/2015/11/Americans-with-Criminal-Records-Poverty-and-Opportunity-Profile.pdf**

Sewell AA, Jefferson KA. 2016. Collateral damage: the health effects of invasive police encounters in New York City. *J. Urban Health* 93(1):42–67

Shannon SK, Uggen C, Schnittker J, Thompson M, Wakefield S, Massoglia M. 2017. The growth, scope, and spatial distribution of people with felony records in the United States, 1948–2010. *Demography* 54(5):1795–818

Sherman L. 2014. Experiments in criminal sanctions: labeling, defiance and restorative justice. *Adv. Criminol. Theory* 18:149–76

Simon J. 2007. *Governing through Crime*: *How the War on Crime Transformed American Democracy and Created a Culture of Fear*. Oxford, UK: Oxford Univ. Press

Sklansky DA. 2018. The problems with prosecutors. *Annu. Rev. Criminol.* 1:451–69

Slobogin C. 2017. Policing, databases, and surveillance. In *Reforming Criminal Justice*: *A Report of the Academy for Justice on Bridging the Gap Between Scholarship and Reform*, ed. E Luna, pp. 209–32. Phoenix, AZ: Acad. Justice

Solove DJ. 2001. Access and aggregation: public records, privacy and the Constitution. *Minn. Law Rev.* 86:1137–209

Solove DJ. 2004. *The Digital Person*: *Technology and Privacy in the Information Age*, Vol. 1. New York: NYU Press

Stevenson M. 2018. Assessing risk assessment in action. *Minn. Law Rev.* 103:303–84

Stuart F. 2016. *Down*, *Out*, *and Under Arrest*: *Policing and Everyday Life in Skid Row*. Chicago: Univ. Chicago Press

Downloaded from www.annualreviews.org. Guest (guest) IP: 172.56.161.251 On: Sat, 24 Oct 2026 22:38:42

Taha v. County of Bucks, 862 F.3d 292 (3d Cir. 2017)

Thomas CW, Bishop DM. 1984. The effect of formal and informal sanctions on delinquency: longitudinal comparison of labeling and deterrence theories. *J. Crim. Law Criminol.* 75(4):1222–45

Uggen C, Stewart R. 2014. Piling on: collateral consequences and community supervision. *Minn. Law Rev.* 99:1871–912

Uggen C, Vuolo M, Lageson S, Ruhland E, Whitham HK. 2014. The edge of stigma: an experimental audit of the effects of low-level criminal records on employment. *Criminology* 52(4):627–54

United States v. Jones, 565 U.S. 400 (2012)

Urban Inst. 2017. *Criminal background checks*: *impact on employment and recidivism*. Rep., Urban Inst., Washington, DC. **https://www.urban.org/sites/default/files/publication/88621/2001174_criminal_background_checks_impact_on_employment_and_recidivism_1.pdf**

US Dep. Justice. 1979. *Privacy and security of criminal history information*: *privacy and the media*. Bur. Justice Stat. Rep., US Dep. Justice, Washington DC. **https://bjs.ojp.gov/content/pub/pdf/pschipm.pdf**

US Dep. Justice. 2001. *Public attitudes toward uses of criminal history*: *a privacy*, *technology*, *and criminal justice information*. Bur. Justice Stat. Rep., US Dep. Justice, Washington, DC. **https://www.bjs.gov/content/pub/pdf/pauchi.pdf**

US Dep. Justice. 2006. *The Attorney General's report on criminal history background checks*. Rep., US Dep. Justice, Washington, DC. **https://bjs.ojp.gov/sites/g/files/xyckuh236/files/media/document/ag_bgchecks_report.pdf**

US Dep. Justice. 2014. *Survey of state criminal history information systems*, *2012*. Bur. Justice Stat. Rep. NCJ 244563, US Dep. Justice, Washington, DC. **https://www.ojp.gov/pdffiles1/bjs/grants/244563.pdf**

Ward DA, Tittle CR. 1993. Deterrence or labeling: the effects of informal sanctions. *Deviant Behav.* 14(1):43–64

Westchester Rockland Newspapers v. Leggett, 48 N.Y.2d 430 (1979)

Western B. 2006. *Punishment and Inequality in America*. New York: Russell Sage Found.

Zuboff S. 2019. *The Age of Surveillance Capitalism*: *The Fight for a Human Future at the New Frontier of Power*. New York: Hachette

Downloaded from www.annualreviews.org. Guest (guest) IP: 172.56.161.251 On: Sat, 24 Oct 2026 22:38:42