CRIMINALLY BAD DATA: INACCURATE CRIMINAL RECORDS, DATA BROKERS, AND ALGORITHMIC INJUSTICE

Sarah Lageson[*]

This Article considers a widely overlooked consequence of having a criminal record in the digital age: the spread of inaccurate or outdated criminal record information. Remarkably common, errors in criminal record data quickly multiply across digital platforms and are nearly impossible for people to manage. Error can begin in governmental sources and spread into the private sector or can be introduced by data aggregators as information across jurisdictions and agencies is compiled into databases and web content. For the subject of the record, error can pose enormous obstacles to securing employment and housing, particularly as automated decision-making and algorithmic governance transform traditional institutional processes. Yet, those who are harmed have very few rights regarding the ability to identify and remedy data error.

Part I of the Article introduces the issue of data error in criminal background checks and describes the scope of the problem. Parts II and III describe how and why criminal record data occurs and detail the specific harms through several theoretical lenses: data error as a due process and equal protection harm, as an informational privacy harm, and as a reputational harm. Part IV analyzes legal obstacles that limit remedies, with a particular focus on the practical obscurity doctrine, the Fair Credit Reporting Act, standing, and various legal immunities available to governments and the private sector. The analysis shows how regulating criminal record data has failed in a digital environment and how existing law fails to protect people from unfounded and illegal discrimination on the basis of inaccurate criminal record information. Part V argues that bad data should be conceptualized under broader critiques of racialized, algorithmic injustice and offers solutions for better regulating and using criminal records.

[*] Associate Professor, Rutgers University-Newark School of Criminal Justice. The author thanks David Noll, Wayne Logan, Eric Goldman, Marty Berger, Vincent Chiao, Hadar Dancig-Rosenberg, Aya Gruber, Itay Ravid, David Alan Sklansky, Jim Francis, and David Lopez for their helpful comments and guidance.

TABLE OF CONTENTS

I. INTRODUCTION

In 2016, Robert McBride was denied a job as a surveyor after a criminal background check reported a series of criminal convictions.[1] But the record was inaccurate and incomplete: his charges had been dismissed.[2] The inaccurate criminal record was sold by a company called the Source for Public Data.[3] Around the same time, another person, Tyrone Henderson, repeatedly asked the Source for Public Data for a copy of his own criminal background check after a string of job rejections also based on faulty data.[4] Here, the company was reporting a felony history that belonged to a *different* Tyrone Henderson in Pennsylvania.[5] This Tyrone Henderson sought a copy of his report to understand what was

[1] Second Amended Class Action Complaint at 24–25, Henderson v. Source for Pub. Data, L.P., 540 F. Supp. 3d 539 (E.D. Va. 2021) (No. 3:20-cv-294).

[2] *Id.*

[3] *Id.* at 12.

[4] *Id.* at 22–23.

[5] *Id.* at 22.

contained in his file and to correct any inaccuracies so that he might be able to secure employment.[6] The Source for Public Data did not respond to his requests.[7]

In the company's view, it had no reason to respond to either Mr. McBride or Mr. Henderson. While such actions are required under the Fair Credit Reporting Act ("FCRA"),[8] The Source for Public Data, it maintained, was not liable under the federal regulations. Instead, they asserted they are immune to liability under Section 230 of the Communications Decency Act.[9] Any error that appears in their database, argued the company, originated in the state's database.[10] They were simply republishing third-party content.

The case turned into a federal class action lawsuit.[11] The plaintiffs, the suit alleged, "have struggled over the last several years with a game of whack-a-mole, in which each time they apply for a job or face a background check, they are confronted with results that are inaccurate and prevent them from moving forward in their lives."[12] But the plaintiffs lost at the district court level after the judge agreed with the defendants that Public Data was immune to liability under Section 230.[13] The appeal came before the Fourth Circuit Court of Appeals in May 2022. At the center was whether data aggregation should fall under the Fair Credit Reporting Act, which would consider criminal record data as "reports" furnished for employers, or if it should fall under Section 230, which would consider criminal record data as simply "data," aggregated for any curious internet user.[14]

The defendants ultimately lost on appeal after the Fourth Circuit found that CDA immunity did not apply.[15] But as the case illustrates, advances in data aggregation have made it increasingly difficult to enforce the fifty-year-old Fair Credit Reporting Act's accuracy standards. In a society increasingly managed by algorithmic governance, the case also raises key questions about who or what is responsible for inaccuracies in the very data used to justify potentially discriminatory hiring or housing determinations.

It's difficult to grasp the level of error across the fragmented governmental and private sector data systems. One analysis of 200 New York state rap sheets

[6] *Id.* at 22–23.

[7] *Id.* at 23.

[8] 15 U.S.C. § 1681g.

[9] Henderson v. Source for Pub. Data, 540 F. Supp. 3d 539, 544 (E.D. Va. 2021), *rev'd*, 53 F.4th 110 (4th Cir. 2022).

[10] Defendants' Memorandum in Support of Motion to Dismiss Plaintiffs' Amended Complaint for Lack of Personal Jurisdiction and Lack of Venue or, in the Alternative, to Transfer Venue at 6, *Henderson*, 540 F. Supp. 3d 539 (No. 3:20-cv-294).

[11] *Henderson*, 540 F. Supp. 3d at 543.

[12] Second Amended Class Action Complaint, *supra* note 1, at 1.

[13] *Henderson*, 540 F. Supp. 3d at 549; Eric Goldman, *Section 230 Preempts Fair Credit Reporting Act (FCRA) Claims-Henderson v. Source for Public Data*, TECH. & MKTG. L. BLOG (May 25, 2021), https://blog.ericgoldman.org/archives/2021/05/section-230-preempts-fair-credit-reporting-act-fcra-claims-henderson-v-source-for-public-data.htm [https://perma.cc/HJU4-Q9MF].

[14] *Henderson*, 540 F. Supp. 3d at 549.

[15] Henderson v. Source for Pub. Data, L.P., 53 F.4th 110, 117 (4th Cir. 2022).

identified an 80% error rate.[16] A federal analysis found that a criminal-background-checking system used for governmental workers incorrectly reported criminal history records for employees 42% of the time.[17] Another empirical study showed that of 101 New Jersey study participants, nearly all had at least one error in a private sector background check.[18] Inaccurate reports constitute the bulk of complaints filed with the Bureau of Consumer Financial Protection; 191,000 such complaints were filed in 2020 alone.[19]

The harms of bad criminal record data are far-reaching due to the ubiquity of background-checking in America. Approximately "94% of employers and about 90% of landlords us[e] background checks to evaluate prospective employees and tenants."[20] First Advantage, Sterling, and Hire Right together produce 56 million background checks a year, and Checkr, which provides background checks for the gig economy, processes 1 million reports each month—about twenty-three reports per minute.[21] From 2009 to 2013, about 120 million criminal record checks were conducted through the Federal Bureau of Investigation for non-criminal justice purposes.[22]

This Article lays out the problem of criminal record error and describes the policy, industry, and technological contexts that facilitate the spread of bad data. The Article then details the specific harms of criminal record error, describes the obstacles that prevent adequate remedy, and closes with a consideration of how

[16] CTR. FOR CMTY. ALTS., BOXED OUT: CRIMINAL HISTORY SCREENING AND COLLEGE APPLICATION ATTRITION 25 n.12 (2015), https://www.communityalternatives.org/wp-content/uploads/2019/11/boxed-out.pdf [https://perma.cc/JD24-2U6U].

[17] Binyamin Appelbaum, *Out of Trouble, but Criminal Records Keep Men Out of Work*, N.Y. TIMES (Feb. 28, 2015), https://www.nytimes.com/2015/03/01/business/out-of-trouble-but-criminal-records-keep-men-out-of-work.html [https://perma.cc/Y2MD-DVAU].

[18] Sarah Lageson & Robert Stewart, *The Problem with Criminal Records: Discrepancies Between Official State Records and Private Sector Background Checks*, 63 CRIMONOLOGY (forthcoming Feb. 2024) (manuscript at 8) (on file with author).

[19] *See* BUREAU OF CONSUMER FIN. PROT., CONSUMER RESPONSE ANNUAL REPORT: JANUARY 1—DECEMBER 31, 2020 22 (2021), https://files.consumerfinance.gov/f/documents/cfpb_2020-consumer-response-annual-report_03-2021.pdf [https://perma.cc/ZSJ6-VA3R]; BUREAU OF CONSUMER FIN. PROT., CONSUMER RESPONSE ANNUAL REPORT: JANUARY 1—DECEMBER 31, 2019 19 (2020), https://files.consumerfinance.gov/f/documents/cfpb_consumer-response-annual-report_2019.pdf [https://perma.cc/N65J-RQ88]; BUREAU OF CONSUMER FIN. PROT., CONSUMER RESPONSE ANNUAL REPORT: JANUARY—DECEMBER 31, 2018 19 (2019), https://files.consumerfinance.gov/f/documents/cfpb_consumer-response-annual-report_2018.pdf [https://perma.cc/R7L8-ATJ4]; BUREAU OF CONSUMER FIN. PROT., CONSUMER RESPONSE ANNUAL REPORT: JANUARY 1—DECEMBER 31, 2017 13 (2018), https://files.consumerfinance.gov/f/documents/cfpb_consumer-response-annual-report_2017.pdf [https://perma.cc/ZPS3-KWAM]; BUREAU OF CONSUMER FIN. PROT., CONSUMER RESPONSE ANNUAL REPORT: JANUARY 1—DECEMBER 31, 2016 18 (2017), https://files.consumerfinance.gov/f/documents/201703_cfpb_Consumer-Response-Annual-Report-2016.PDF [https://perma.cc/D3A3-NSMQ].

[20] ARIEL NELSON, NAT'L CONSUMER L. CTR., BROKEN RECORDS REDUX: HOW ERRORS BY CRIMINAL BACKGROUND CHECK COMPANIES CONTINUE TO HARM CONSUMERS SEEKING JOBS AND HOUSING 3 (2019), https://www.nclc.org/wp-content/uploads/2022/09/report-broken-records-redux.pdf [https://perma.cc/K87F-CDVL].

[21] *Id.* at 7.

[22] U.S. GOV'T ACCOUNTABILITY OFF., GAO-15-162, CRIMINAL HISTORY RECORDS: ADDITIONAL ACTIONS COULD ENHANCE THE COMPLETENESS OF RECORDS USED FOR EMPLOYMENT-RELATED BACKGROUND CHECKS 1 (2015), https://www.gao.gov/assets/gao-15-162.pdf [https://perma.cc/MZ35-RZHS].

things might improve, particularly if criminal record error is framed as a racial injustice issue in the algorithmic age.

The complexity of the law and extremely limited remedies available for people who have been harmed by error invites a broader critique of ostensibly neutral, data-driven processes that underlie today's criminal background check. Accuracy is one lens to question the efficacy of a system that too often relies on inaccurate information derived from a historically racialized system and then uses this information to deny access to housing, education, employment, and social and digital life. The Article ultimately argues that bad data should become a central critique of our current regime of algorithmically derived discrimination.

II. TYPES OF CRIMINAL RECORD ERROR

A. Governmental Error

Criminal record data error is surprisingly common but is difficult to define.[23] Error can consist of factually inaccurate criminal record data via a mismatched identity or incorrectly entered police or court data that create a false criminal record for a person. Error can reflect missing information (such as a missing case disposition) that implies a case is still pending, open, or unresolved. Error can also reflect the erroneous reporting of criminal record information not meant to be publicly disclosed, such as in reporting juvenile records or cases that have been sealed, expunged, or pardoned.

At the governmental level, each branch of the criminal justice system maintains individual data systems, so errors can originate from a multitude of sources.[24] Even before the advent of digital records, experts warned of data fallibility, noting that "[t]he accuracy and completeness of criminal history record information—the quality of data in those records—has emerged as perhaps the most significant information issue confronting the criminal justice community."[25]

In a case related to the 4th Amendment's exclusionary rule in 2009, Justice Ruth Bader Ginsburg warned that while "[e]lectronic databases form the nervous system of contemporary criminal justice operations . . . [t]he risk of error stemming from these databases is not slim."[26] Indeed, she pointed out, "law enforcement databases are insufficiently monitored and often out of date" and "[i]naccuracies in expansive, interconnected collections of electronic information raise grave concerns for individual liberty."[27] A loss of fundamental constitutional

[23] *See* Wayne A. Logan & Andrew Guthrie Ferguson, *Policing Criminal Justice Data*, 101 MINN. L. REV. 541, 542–43, 545 (2016).

[24] *See* SARAH ESTHER LAGESON, DIGITAL PUNISHMENT: PRIVACY, STIGMA, AND THE HARMS OF DATA-DRIVEN CRIMINAL JUSTICE 19 (2020).

[25] SEARCH GRP., INC., U.S. DEP'T OF JUST. BUREAU OF JUST. STATS., CRIMINAL JUSTICE INFORMATION POLICY: DATA QUALITY OF CRIMINAL HISTORY RECORDS (1985), https://bjs.ojp.gov/content/pub/pdf/dqchr.pdf [https://perma.cc/V4JR-6UCV].

[26] Herring v. United States, 555 U.S. 135, 155 (2009) (Ginsburg, J., dissenting).

[27] *Id.*

rights can flow from a database error;[28] Justice Ginsburg further noted the propensity for errors to cause grave harm, as "computerization greatly amplifies an error's effect, and correspondingly intensifies the need for prompt correction; for inaccurate data can infect not only one agency, but the many agencies that share access to the database."[29]

Differences in data collection practices among criminal justice agencies also lead to data quality problems as data are aggregated—while state police "rap sheets" may be organized by fingerprint or social security number, easier-to-access criminal court records might only provide names and dates of birth.[30] People with common names are especially susceptible to data matching problems, such as a "Mark Johnson" in Cleveland who was not only mislabeled as having been convicted of a sex offense but also as a person with a drug conviction in a completely different background check for a different job a year earlier.[31]

Different types of public policies also guide the relative privacy or disclosure of the different types of criminal record information produced by various agencies, even within states.[32] An empirical policy analysis finds that most states regulate the release of arrest information through public records laws, while state common law allows disclosure of criminal court records (which contain a different set of criminal history information often unlinked from law enforcement data).[33] Conversely, state administrative law often regulates the release of correctional information about people who are incarcerated, with a blend of penal law and administrative law guiding the release of conviction records (also known as RAP sheets).[34] This means that, for the criminal record subject, different versions of their criminal record may exist between agencies that are also disseminated to the public in varying channels and with varying degrees of completeness. This, in turn, increases the likelihood of data error, encourages the sharing of pre-conviction records through the greater disclosures of arrest and charging information (as opposed to the relatively closed nature of conviction summaries), and, in effect, creates multiple channels for data aggregators to obtain information.

Governmental agencies also face difficulties in matching data across different parts of the system, such as between police departments, criminal courts, and probation offices, which can lead to factual error as data gathered and

[28] Herring v. United States, 555 U.S. 135, 147–48 (2009); *see also* Arizona v. Evans, 514 U.S. 1, 14 (1995).

[29] Arizona v. Evans, 514 U.S. 1, 28 (1995) (Ginsburg, J., dissenting).

[30] Olivera Perkins, *Errors in Background Checks Cost Job Seekers*, CLEVELAND.COM (Dec. 15, 2012, 7:20 PM), https://www.cleveland.com/business/2012/12/job_applicants_lose_out_as_err_1.html [https://perma.cc/LP9X-MTMT].

[31] *Id.*

[32] Juan R. Sandoval & Sarah E. Lageson, *Patchwork Disclosure: Divergent Public Access and Personal Privacy Across Criminal Record Disclosure Policy in the United States*, 44 LAW & POL'Y 255, 257 (2022).

[33] *Id.* at 263–65.

[34] *Id.* at 266–67.

maintained by separate agencies do not transfer properly.[35] One consequence of poorly integrated data systems is missing case dispositions, where the final disposition of an arrest or criminal charge remains unresolved. Missing dispositions range from 22% of all arrest records in Massachusetts to 98% in Iowa, with a national mean of 69%.[36] Two states (Virginia and West Virginia) still use paper-based methods to report case dispositions to the FBI repository.[37] Several states take more than a year to update the central state repository after a court finalizes a case disposition.[38] A recent study in California found that 35% of criminal cases were missing a final disposition in statewide rap sheet data, and 75% of people had at least one such incomplete case on their record.[39] There have been efforts to improve the reporting of case dispositions. In 2009, for instance, the FBI's Advisory Policy Board created a Disposition Task Force, which helped raise disposition rates for several states[40] but failed to create national standards for collecting and reporting disposition information.[41] The Department of Justice assisted states in improving criminal history systems through $23 million in state grantmaking from 2008 to 2012, but missing and incomplete records persist.[42]

Missing case dispositions can be quite harmful.[43] First, while missing dispositions for recent felony cases may reflect a case still in process,[44] empirical analyses of criminal record error show that missing dispositions can linger for years or decades, even if a case was dismissed.[45] Second, the burden of fixing missing case dispositions is most often shouldered by the record subject, who often must physically visit the courthouse where the case was initiated and request and/or pay for disposition paperwork.[46] Third, if an employment offer is contingent on a clear background check, the employer may move on to additional

[35] *See, e.g.*, U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 22, at 27 ("Senior officials in 3 of our 4 case study states said that they faced challenges in transferring unique case control numbers among local criminal justice agencies—such as law enforcement agencies, courts, prosecutors, and the state record repository.").

[36] *See* SEARCH GRP., INC., U.S. DEP'T OF JUST. BUREAU OF JUST. STATS., SURVEY OF STATE CRIMINAL HISTORY INFORMATION SYSTEMS, 2020, tbl.1 (2022), https://www.ojp.gov/pdffiles1/bjs/grants/305602.pdf [https://perma.cc/VT8X-99QH].

[37] *Id.* at 7 ("Two states (Virginia and West Virginia) sent 100% of their final case dispositions to the FBI via hard copy or paper.").

[38] *See id.* at tbl.7b.

[39] Alyssa C. Mooney, Alissa Skog & Amy E. Lerman, *Racial Equity in Eligibility for a Clean Slate Under Automatic Criminal Record Relief Laws*, 56 LAW & SOC'Y REV. 398, 413 (2022).

[40] *See, e.g.*, U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 22, at 18 ("BJS surveys show that the number of states that reported providing more than 75 percent of their arrest records with final dispositions increased from 16 states in 2006 to 20 states in 2012.").

[41] *See id.* at 25.

[42] *Id.* at 22.

[43] Amy Myrick, *Facing Your Criminal Record: Expungement and the Collateral Problem of Wrongfully Represented Self*, 47 LAW & SOC'Y REV. 73, 85 (2013).

[44] *See* U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 22, at 19–20.

[45] Lageson & Stewart, *supra* note 18 (manuscript at 16); *see also* U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 22, at 26 ("According to officials from DOJ and our case study states, one of the major contributors to arrest records not having final dispositions occurs when prosecutors decline to prosecute an individual but do not report this information to the state's central records repository.").

[46] *See* LAGESON, *supra* note 24, at 22.

candidates while the missing disposition is being resolved by the applicant.[47] And perhaps most importantly, these mismatched, fragmented, and unresolved criminal history records are duplicated into private sector databases, where they become even more difficult to trace and remedy.

B. Private Sector Error

Governmental errors spread into private sector databases through data aggregation, "blending public and private systems that can mask the sources of error," leading to mismatched reports, the reporting of sealed or expunged records, and a failure to properly categorize incidents, such as reporting a single arrest numerous times or classifying crimes incorrectly.[48] Actual estimates of error in private sector databases are unknown and difficult to track.[49] Many people are unaware of what data are contained in the potentially thousands of criminal record sources available to background-checking companies, landlords, and employers, and will only file a complaint if an adverse action is taken against them and they then uncover the error.[50]

Many courts directly sell information to data brokers, increasing the likelihood that error spreads across platforms.[51] Local governments also routinely post criminal record information directly to the internet, including arrest rosters, jail populations, criminal court defendants, and people incarcerated in state prisons.[52] Once posted online, the proverbial bell cannot be unrung.[53] Web scraping, the automated extraction of information posted to websites,[54] allows public criminal records to become a valuable bulk data source for data brokers and third-party websites that aggregate and repost criminal record information for public use and for-profit enterprises.[55]

Data scrapers extract publicly available data for uses as varied as data-driven journalism, social science research, aggregating news and other useful public information, and refining marketing techniques.[56] The practice is widespread; LinkedIn blocks approximately 95 million automated attempts to scrape data every day.[57] Other scraping purposes have been viewed more critically, such as the company Clearview AI's scraping of social media content to create

[47] U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 22, at 20.

[48] Logan & Ferguson, *supra* note 23, at 562.

[49] NELSON, *supra* note 20, at 16.

[50] *Id.*

[51] *See, e.g.*, HARRIS COUNTY CLERK'S OFFICE, https://www.cclerk.hctx.net/applications/websearch/ (last visited July 23, 2023) [https://perma.cc/A3Q5-D3EP] (showing a Texas court website that provides a link for the "data sales" desk that handles bulk data inquiries).

[52] LAGESON, *supra* note 24, at 6.

[53] *See* Alexander Tsesis, *Data Subjects' Privacy Rights: Regulation of Personal Data Retention and Erasure*, 90 U. COLO. L. REV. 593, 597 (2019).

[54] Andrew Sellars, *Twenty Years of Web Scraping and the Computer Fraud and Abuse Act*, 24 B.U. J. SCI. TECH. L. 372, 373 (2018).

[55] LAGESON, *supra* note 24, at 8.

[56] *See generally* Andrew M. Parks, Note, *Unfair Collection: Reclaiming Control of Publicly Available Personal Information from Data Scrapers*, 120 MICH. L. REV. 913 (2022).

[57] hiQ Labs, Inc. v. LinkedIn Corp., 31 F.4th 1180, 1186 (9th Cir. 2022).

massive sets of personal data for facial recognition technologies sold to law enforcement.[58] The notorious mugshot industry scrapes booking photos from governmental websites and reposts them on websites,[59] spoiling digital reputations and stigmatizing millions of people who are arrested each year.[60] Courts have held that scraping personal information is allowable as long as the information is publicly accessible.[61] Criminal record data can thus be lawfully redisseminated by third parties if it were lawfully obtained, publicly available, and truthful, following *Smith v. Daily Mail Publishing Co.*[62]

Data brokers—"companies that collect consumers' personal information and resell or share that information with others"[63]—both exacerbate criminal record error introduced at the state level and create new error through sloppy data matching techniques by failing to regularly update criminal record information, and by reselling erroneous criminal record information to other data vendors and background check companies.[64] The Federal Trade Commission has made "call[s] for transparency and accountability" in the data brokerage industry, noting how it is a "complex" industry with "multiple layers of data brokers providing data to each other" to make inferences about people (such as categories that focus on race and income), then sharing and selling this information without the consent or knowledge of data subjects and by operating with a "fundamental lack of transparency."[65] In 2012, the National Consumer Law Center testified to the Senate Subcommittee on Consumer Protection, Product Safety, and Insurance that companies specializing in criminal background checks are "not required to be licensed or even registered, nor is there any one source identifying all of these companies. . . . [T]here is no centralized location to obtain the kind of information required to determine the accuracy of the information these agencies are collecting."[66]

Sometimes referred to as "zombie" records,[67] data brokers (and the screening companies that buy and use their data products) often report factually

[58] Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, N.Y. TIMES (Nov. 2, 2021), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html [https://perma.cc/K6HF-VYZ8].

[59] Eumi K. Lee, *Monetizing Shame: Mugshots, Privacy, and the Right to Access*, 70 RUTGERS U. L. REV. 557, 560 (2018).

[60] Sarah E. Lageson, Elizabeth Webster & Juan R. Sandoval, *Digitizing and Disclosing Personal Data: The Proliferation of State Criminal Records on the Internet*, 46 LAW & SOC. INQUIRY 635, 636 (2021).

[61] *hiQ Labs, Inc.*, 31 F.4th at 1189.

[62] Smith v. Daily Mail Publ'g Co., 443 U.S. 97, 105–06 (1979).

[63] U.S. FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY 1 (2014).

[64] Logan & Ferguson, *supra* note 23, at 559–63.

[65] U.S. FED. TRADE COMM'N, *supra* note 63, at 46, 49.

[66] *Credit Reports: What Accuracy and Errors Mean for Consumers: Hearing Before the S. Subcomm. on Consumer Protection, Product Safety, and Ins., S. Comm. on Com., Sci., and Transp.*, 113th Cong. (2013) (statement of Ira Rheingold, Executive Director, National Association of Consumer Advocates also on behalf of National Consumer Law Center).

[67] Lauren Kirchner, *When Zombie Data Costs You a Home*, MARKUP (Oct. 6, 2020, 8:00 AM), https://themarkup.org/locked-out/2020/10/06/zombie-criminal-records-housing-background-checks [https://perma.cc/B5KQ-8S6S]; *Watch Out for Zombie Records! Yours Can Hurt You.*, KAN. LEGAL SERVS. (June

incorrect criminal record information or mistakenly report expunged or sealed records.[68] While it is nearly impossible to establish inaccuracy rates in the private sector, a 2004 study by the National Association of State Public Interest Groups conducted a survey that found 54% of credit reports contained incorrect identity information and 79% contained at least one serious error.[69] The FTC estimates that over 40 million consumers have an error on a credit report.[70] While criminal background checks perform a slightly different function, consumer reports routinely provide both criminal and credit score information.[71]

Sometimes, a private background check is simply provided for the wrong person in the database, particularly if they have a common name and the company is using basic matching criteria to generate reports, such as name, sex, and city of residence (as is common in the industry).[72] While some of the larger CRAs have made efforts to use more sophisticated matching criteria, many other CRAs seek to cut costs and maintain a competitive edge by relying on "fuzzy logic" matching.[73] To further complicate matters, companies may inadvertently assign incorrect identifiers to people in efforts to merge and match datasets; for instance, assigning a social security number to the wrong person and then using that very same social security number to generate factually inaccurate results.[74]

Criminal record data are constantly changing as cases are dismissed or sealed—but these changes in governmental databases often are not reflected in private sector databases. Clean Slate reforms are sweeping the United States, allowing for the sealing or expungement of potentially millions of criminal records.[75] But for people to leverage the benefits of criminal record expungement, private companies must comply with updating their records. Automatic record clearance is also done without the knowledge of the record subject and is processed in batch court orders—which means private repositories must constantly refresh their data.[76] It is clear this is not happening.[77] Sharon Dietrich of

2022) https://www.kansaslegalservices.org/node/2531/watch-out-zombie-records-yours-can-hurt-you [https://perma.cc/8FCA-PA6Q]; Alessandro Corda & Sarah E. Lageson, *Disordered Punishment: Workaround Technologies of Criminal Records Disclosure and the Rise of a New Penal Entrepreneurialism*, 60 BRIT. J. CRIMINOLOGY 245, 258 (2020).

[68] *Reporting Expunged or Sealed Cases in Commercial Background Checks Violates the Fair Credit Reporting Act*, CMTY. LEGAL SERVS. OF PHILA. (Feb. 9, 2018), https://clsphila.org/criminal-records/fcra-and-expungements/ [https://perma.cc/DAX7-2KA8].

[69] ALISON CASSADY & EDMUND MIERZWINSKI, MISTAKES DO HAPPEN: A LOOK AT ERRORS IN CONSUMER CREDIT REPORTS 4 (2004).

[70] *Is My Credit Report Accurate? For Over 40 Million Americans, the Answer Is No*, AM. BANKR. INST., https://www.abi.org/feed-item/is-my-credit-report-accurate-for-over-40-million-americans-the-answer-is-no#:~:text=According%20to%20a%20recent%20study,of%20the%20entire%20national%20population (last visited Mar. 23, 2023) [https://perma.cc/S3WF-7S9W].

[71] *Using Consumer Reports: What Landlords Need to Know*, U.S. FED. TRADE COMM'N (Oct. 2016), https://www.ftc.gov/business-guidance/resources/using-consumer-reports-what-landlords-need-know [https://perma.cc/7HMS-6Z9W].

[72] Williams v. First Advantage LNS Screening Sols., Inc., 155 F. Supp. 3d 1233, 1238 (N.D. Fla. 2015).

[73] NELSON, *supra* note 20, at 17–18.

[74] *Id.* at 19.

[75] *See* Mooney et al., *supra* note 39, at 400.

[76] *See* NELSON, *supra* note 20, at 19.

[77] *Id.*

Philadelphia's Community Legal Services refers to expunged records as "ants under the refrigerator" and warns clients to be alert to their expunged record showing up in background checks, citing an example of one client whose expunged records were still appearing in background checks twenty months after the expungement order.[78] As she describes it, "people who were counting on the fresh start promised by the expungement procedure are frustrated, and may have experienced a major life setback as a result."[79] These very concerns may help explain the relatively low uptake of criminal record expungement petitions.[80] The disclosure of juvenile records—either because of permissive or conflicting state guidelines or by inadvertent disclosure—also undermines the rehabilitative aims of a system that, in part, relies on the confidentiality of records. Once released into the private data market, these records, too, suffer data error.[81]

Given the many potential sources of criminal record data and opportunities for data error, courts have struggled to define data "accuracy" in the background checking context, taking either a "technical" accuracy standard (where the report is factually correct but may be misleading or incomplete in some respect) or a "maximum possible accuracy" approach (finding a background check as inaccurate if it is either patently incorrect or misleading enough to be expected to create an adverse outcome).[82] This might include listing cases that do not have a final disposition (and failing to follow up with the court directly to complete the record), including multiple entries related to a single arrest or charge that implies a "repeat offender" and exaggerates the seriousness of a record, or a screening company miscategorizing the severity of a criminal record, such as reporting a misdemeanor as a felony or inaccurately characterizing certain traffic offenses and criminal convictions.[83] Additionally, an applicant who has a misleading or inaccurate criminal history report will appear as a liar if the potential employer or landlord asks them for more detail and the applicant answers in a manner that differs from the written report.[84] Interviews with employers demonstrate how confusing and unclear criminal records lead to "legal ambiguity" that may trigger more employment discrimination based on a criminal record, just one of many potential harms.[85]

[78] Sharon M. Dietrich, *Ants Under the Refrigerator? Removing Expunged Cases from Commercial Background Checks*, 30 AM. BAR ASS'N CRIM. JUST. 26, 28 (2016).

[79] *Id.* at 54.

[80] J.J. Prescott & Sonja B. Starr, *Expungement of Criminal Convictions: An Empirical Study*, 133 HARV. L. REV. 2460, 2488–90 (2020).

[81] *Safeguarding the Confidentiality of Youth in the Justice System: Recommendations and Resources*, NAT'L JUV. JUST. NETWORK (Aug. 2016), http://www.njjn.org/our-work/confidentiality-of-youth-in-justice-system-safeguards#dagger [https://perma.cc/W9GL-KEVF].

[82] Noam Weiss, Note, *Combating Inaccuracies in Criminal Background Checks by Giving Meaning to the Fair Credit Reporting Act*, 78 BROOK. L. REV. 271, 286 (2012).

[83] NELSON, *supra* note 20, at 21.

[84] Jenny Roberts, *Expunging America's Rap Sheet in the Information Age*, 2015 WIS. L. REV. 321, 341 (2015).

[85] Sarah Esther Lageson, Mike Vuolo & Christopher Uggen, *Legal Ambiguity in Managerial Assessments of Criminal Records*, 40 LAW & SOC. INQUIRY 175, 176–77 (2015).

III. Harms of Criminal Record Error

Criminal record data error introduces several concrete harms, including due process and equal protection harms, informational privacy harms, and reputational harms. Part of this is cultural: in America, criminal records are routinely used to stigmatize and discriminate in both formal and informal settings, such as employment, housing, volunteering, and in social contexts like online dating and networking.[86]

A. Due Process and Equal Protection

Inaccurate criminal records deny people due process. Sloppy and inconsistent data collection and aggregation practices create procedural due process violations, while the stigmatizing mark of inaccurate criminal records creates substantive due process problems.

Due process encompasses the constitutional requirement in the Fifth Amendment that any governmental deprivation of liberty or property be preceded by notice and the opportunity to be heard.[87] Because criminal records have largely been considered records of the *state*, not of the individual record subject, due process considerations have been largely overlooked.[88]

Yet, it is increasingly clear that the criminal record itself leads to significant deprivations of liberty and property. This invites the argument that disseminating criminal record "big data" requires specific data-privacy-related due process protections outside what is traditionally offered to criminal defendants.[89] As of now, record subjects have virtually no control over the types of personal information collected by the state and later released to the private sector, little ability to ensure data quality or proactively check for erroneous data, and no option to opt out of the dissemination of personal information contained in criminal records, such as their name, photograph, or home address—even if they were never convicted of a crime.[90] As automated decision-making regimes that use criminal records replace traditional institutionalized domains of procedural due process, data error becomes more difficult to locate even as it produces unfair outcomes.[91] This highlights the need for "big data procedural due process" to encourage notice and accuracy within the private sector as well.[92]

The unregulated spread of criminal record information, particularly arrest and charging information released prior to a criminal conviction, also violates the presumption of innocence. This is particularly harmful when the public

[86] *See generally, e.g.*, Devah Pager, *The Mark of a Criminal Record*, 108 AM. J. SOCIO. 937 (2003).

[87] U.S. CONST. amend. V; Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, 55 B.C. L. REV. 93, 112 (2014).

[88] *See* Jeffrey Selbin, Justin McCrary & Joshua Epstein, *Unmarked? Criminal Record Clearing and Employment Outcomes*, 108 J. CRIM. L. & CRIMINOLOGY 1, 4 (2018).

[89] Crawford & Schultz, *supra* note 87, at 113.

[90] *Id.* at 108.

[91] Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249, 1267 (2007).

[92] Crawford & Schultz, *supra* note 87, at 124–28.

criminal record erroneously assigns public guilt to an individual, and this information is readily available to the general public. Because it can be nearly impossible for the subject of the record to locate the original error, as well as all the digital spaces that now replicate the error, they may be effectively and incorrectly "marked" as a criminal in the public sphere.

An equal protection lens is also worth considering. Data error has a disparate impact on communities already most harmed by policing and prosecution.[93] Racial disproportionately is undisputed in the criminal legal system and often emerges through discretionary policing, prosecutorial, and judicial decision-making. Criminal records reify these racial inequalities, which are further exacerbated by racialized patterns of data integrity problems, a concept sociologist David McElhattan calls "punitive ambiguity."[94] I return to this issue in Part V.

Data error also undermines criminal legal system reform efforts meant to ameliorate the detrimental effects of criminal records, such as expungement, Clean Slate, and pretrial diversion programs.[95] Inaccurate records are complicating efforts to automate criminal record expungement because no algorithm can overcome incomplete and missing data,[96] and so the legislative remedy of providing a "clean slate" to people who have old convictions is dramatically curtailed by data integrity problems.[97]

B. Reputational and Privacy Harms

There is ample evidence that incorrect criminal background checks lead to social and reputational harm. Journalistic coverage describes scenarios where people are offered a job only to have the offer rescinded after a faulty background check erroneously labels a person as a convicted criminal—an error that can take years to remedy.[98] In Tennessee, a person lost a coveted spot on a subsidized housing waitlist after being misidentified as having a sex offense conviction.[99] The Society for Human Resources Management similarly warned of a Pennsylvania man barred from employment due to a faulty criminal background check rooted in a data broker's strategy of providing the recipient of a background check with a set of "possible matches."[100] The article recounts the emotional experience of being wrongly identified in a criminal background check and

[93] Logan & Ferguson, *supra* note 23, at 569.

[94] *See generally* David McElhattan, *Punitive Ambiguity: State-Level Criminal Record Data Quality in the Era of Widespread Background Screening*, 24 PUNISHMENT & SOC'Y 367 (2021).

[95] LAGESON, *supra* note 24, at 10.

[96] *See* Mooney et al., *supra* note 39, at 413.

[97] Colleen Chien, *America's Paper Prisons: The Second Chance Gap*, 119 MICH. L. REV. 519, 520 (2020).

[98] Perkins, *supra* note 30.

[99] Steven Melendez, *When Background Checks Go Wrong*, FAST CO. (Nov. 17, 2016), https://www.fastcompany.com/3065577/when-background-checks-go-wrong [https://perma.cc/78S2-EAU7].

[100] Dori Meinert, *Search and Verify: Why Criminal Background Checks May Not Be as Accurate as You Think*, SHRM (Dec. 1, 2012), https://www.shrm.org/hr-today/news/hr-magazine/pages/1112-criminal-background-checks.aspx [https://perma.cc/ML3C-DBB6].

navigating the negative responses such a label brings, where the wrongly identified person described being nervous, upset, angry, and shocked.[101]

Criminal record information is popular across the internet, including mugshot galleries and unregulated "people search" websites that simply aggregate bulk public criminal record information without ensuring accuracy.[102] The popularity of such websites firmly entrenches criminal record information into the top search results for a person's name, even if the underlying criminal record information is incorrect.

Criminal record data might also be viewed through an informational privacy lens. The constitutional right to informational privacy is related to Justice Brandeis's "right . . . to be let alone," or as privacy expert Alan Westin defined it in 1967, the ability of people "to determine for themselves when, how, and to what extent information about them is communicated to others."[103]

Scholars and advocates have long been concerned with privacy rights in the big data era,[104] but less attention has directly centered on criminal records as a source of an informational privacy violation. That said, broader approaches to regulating personal data are applicable to the criminal records context. Several U.S. government agencies have released FIPPs, or Fair Information Practice Principles, that derive from the Privacy Act of 1974 and explicitly include recommendations for data quality and integrity.[105] While much of this discussion has centered on the use of consumer data, these arguments can be easily extended to criminal records, especially as criminal records become increasingly managed by and accessed through the private sector.

C. Immigration

Criminal records are also becoming increasingly central to immigration proceedings, including both removal proceedings and affirmative applications to acquire lawful status.[106] Inaccurate or mismatching criminal record information can delay immigration court processing and lead the agency to adjudicate in their discretion against the immigrant rather than wait for paperwork to be collected and supplied.[107] USCIS has also increased the amount of information required to explain a criminal justice system interaction, such as by requiring applicants to supply the agency with police and arrest records underlying even those events that did not lead to a conviction and even if the immigrant was a crime victim.[108] Plus, going into a police station or courthouse to obtain paperwork to remedy

[101] *Id.*

[102] LAGESON, *supra* note 24, at 29.

[103] *Id.* at 32.

[104] *See* Crawford & Schultz, *supra* note 87, at 93.

[105] The Privacy Office, *The Fair Information Practice Principles at Work*, U.S. DEP'T OF HOMELAND SEC. (June 2011), https://www.dhs.gov/sites/default/files/publications/dhsprivacy_fippsfactsheet.pdf [https://perma.cc/Y5YK-8YHB].

[106] Erica D. Rosenbaum, Note, *Relying on the Unreliable: Challenging USCIS's Use of Police Reports and Arrest Records in Affirmative Immigration Proceedings*, 96 N.Y.U. L. REV. 256, 256 (2021).

[107] *Id.* at 259.

[108] *Id.*

inaccurate or missing criminal records further puts an undocumented person at risk of being detained by ICE.[109] In removal proceedings, "a noncitizen's eligibility to apply for relief from removal hinges on state and local recordkeeping practices."[110] Incomplete and inaccurate criminal records, developed for local recordkeeping purposes, are then repurposed as an allegedly reliable indicator for removal proceedings, even if they are replete with missing or confusing information that immigration judges must puzzle together at their discretion—leading to "inconsistent and potentially unjust immigration outcomes."[111] ICE also subscribes to private sector criminal record databases, such as Thomson Reuters' CLEAR database, further subjecting people under immigration surveillance to potentially inaccurate data.[112]

D. Systems Avoidance and Procedural Justice

Inaccurate criminal records have real-world consequences for people's ability to live a full life.

Empirical social science research has shown that having a criminal record is related to "systems avoidance,"[113] and inaccuracies contribute to "digital avoidance," wherein people who are confronted with multiple, messy versions of their criminal record purposefully opt out of institutional scenarios that require a background check.[114] This leads people away from improved economic, social, and living conditions and could contribute conversely to decreasing public safety by increasing recidivism risk.[115]

Inaccurate records also erode confidence in the system, increase perceptions of unfair treatment, and may decrease procedural justice. Procedural justice research has shown that people care deeply about the information about them that is used to adjudicate a decision, which thus indicates whether the outcome or treatment was deserved.[116] Inaccurate information is especially harmful for procedural justice purposes when that bad data leads to police profiling through wrongful inclusion in a gang database or the denial of an apartment or job due to a faulty background check. The experience of contending with one's own criminal record, particularly when it contains incorrect information, constitutes a

[109] *Should I Clear My Criminal Record for Immigration Purposes?*, ILL. LEGAL AID ONLINE (July 12, 2022), https://www.illinoislegalaid.org/legal-information/will-clearing-my-juvenile-record-help-my-immigration-case [https://perma.cc/4T6A-9K4U].

[110] Brief of National Association of Criminal Defense Lawyers & National Association of Federal Defenders as Amicus Curiae at 2, Pereida v. Wilkinson, 141 S. Ct. 754 (2021) (No. 19-438).

[111] *Id.* at 3.

[112] Brooks v. Thomson Reuters Corp., No. 21-CV-01418-EMC, 2021 WL 3621837, at *1 (N.D. Cal. Aug. 16, 2021).

[113] Sarah Brayne, *Surveillance and System Avoidance: Criminal Justice Contact and Institutional Attachment*, 79 AM. SOCIO. REV. 367, 367 (2014).

[114] LAGESON, *supra* note 24, at 9.

[115] Sarah E. Lageson & Shadd Maruna, *Digital Degradation: Stigma Management in the Internet Age*, 20 PUNISHMENT & SOC'Y 113, 124 (2018).

[116] Steven L. Blader & Tom R. Tyler, *A Four-Component Model of Procedural Justice: Defining the Meaning of a "Fair" Process*, 29 PERSONALITY & SOC. PSYCH. BULL. 747, 747 (2003).

form of "wrongful representation" that contributes to inequalities precisely because records hold so much power relative to the subject's ability to correct the information.[117]

E. Automated Decision-Making

Bad data matter for contexts far broader than a background report for a single applicant ordered by a landlord or employer. Now, personal data—including criminal records—are part of a broader and deeper system of algorithmic governance that uses automated decision-making in domains of life. Data power outcomes in setting bail or making pretrial determinations, in directing police attention, and in lending decisions and loan rates.[118] Because these algorithmic decisions exist in a black box, protected by proprietary technologies, it is nearly impossible for someone to know whether or not erroneous data are being leveraged against them.[119]

Increasingly automated systems of matching and searching enormous swaths of data in efforts to produce background checks more quickly than competitors and to cut costs associated with human review.[120] Background check screeners then claim that the elimination of human review creates more objective reporting—the company Checkr, for instance, claims on its website that its "AI-powered technology" will "reduce time, human error, and bias from manual reviews."[121]

Automated decision-making further obscures data error when a screening company assigns a "score" to the subject of a check and provides that information to the requester.[122] The National Consumer Law Center ("NCLC") warns of the risks associated with these approaches, as "[i]n situations where the background screener provides an eligibility determination, the landlord or employer often does not receive or review the underlying background check report, let alone the underlying records."[123] In a report on criminal record errors in the private sector, the NCLC described a housing discrimination case where a landlord relied on an automated decision from a screening company and denied a tenant an apartment based on her disabled son's supposed (but unspecified) criminal history—which turned out to be a single non-conviction retail theft charge.[124] The landlord, lacking any specific information about the nature of the record, simply disqualified the potential renters.[125]

[117] Myrick, *supra* note 43, at 102.

[118] Blader & Tyler, *supra* note 116, at 747.

[119] *See generally* Candice Schumann, Jeffrey S. Foster, Nicholas Mattei & John P. Dickerson, *We Need Fairness and Explainability in Algorithmic Hiring*, INT'L CONF. ON AUTONOMOUS AGENTS & MULTI-AGENT SYS. (2020), https://www.cs.tufts.edu/~jfoster/papers/aamas20.pdf [https://perma.cc/4HW2-5CR7].

[120] NELSON, *supra* note 20, at 9–10.

[121] *See* CHECKR, https://checkr.com/ (last visited July 23, 2023) [https://perma.cc/LE6T-QUSR].

[122] NELSON, *supra* note 20, at 12–13.

[123] *Id.* at 13.

[124] *Id.* (citing Conn. Fair Hous. Ctr. v. Corelogic Rental Prop. Sols., LLC, 369 F. Supp. 3d 362, 367–68 (D. Conn. 2019)).

[125] *Id.*

The widespread problem of criminal record error has been approached through a variety of strategies at local, state, and federal levels. Still, problems persist. This begs the question of how criminal record data should be regulated and managed in the digital age, where a criminal record has now become part of a broader personal data ecosystem.

IV. OBSTACLES TO REMEDY

Contending with an erroneous criminal record can be difficult, confusing, time-consuming, and ultimately futile due to the constellation of information kept in distinct databases. Legal frameworks exacerbate these practical barriers; in particular, legal doctrines designed to improve accuracy are poorly designed for the big data age and are overshadowed by the legal immunities that protect the governments and companies that provide bad data.

A. The Demise of Practical Obscurity

Before the internet became part of daily life and data aggregation was possible at today's scale, criminal record privacy was understood through the lens of "practical obscurity," rooted in the hassle of tracking down police and court records kept on paper.[126] Some privacy scholars have argued that obscurity operates as a protective barrier to the digital surveillance state, framing obscurity as representing "transaction costs involved in finding or understanding information."[127]

Practical obscurity also helped obscure—and limit the harms of—criminal record error. According to one observer,

> [p]ractical obscurity helped ameliorate the criminal justice system's harshness. Mistaken records existed, names and dates of birth were confused, but the obscurity of the record made it unlikely that errors would harm innocent people. Mistakes were also correctable using a bottle of White-Out [on the single record that contained erroneous information]; today, the same sorts of mistakes are replicated endlessly on Internet-connected computers worldwide.[128]

The Supreme Court developed the concept of practical obscurity by finding that a privacy interest exists when public information is difficult to obtain—in this case, a person's rap sheet.[129] Tellingly, the case emerged from broader social, political, and technological debates about a newly computerized society in the 1960s to 1980s.[130] In a 1986 article prescient of today's data brokerage

[126] Woodrow Hartzog & Evan Selinger, *Surveillance as Loss of Obscurity*, 72 WASH. & LEE L. REV. 1343, 1356 (2015).

[127] *Id.* at 1345–46.

[128] Robert Sykora, *The Invisible Worm and the Presumption of Guilt,* 37 WM. MITCHELL L. REV. 722, 727 (2011).

[129] Patrick C. File, *A History of Practical Obscurity: Clarifying and Contemplating the Twentieth Century Roots of a Digital Age Concept of Privacy*, 6 U. BALT. J. MEDIA L. ETHICS 4, 5 (2017).

[130] *Id.* at 6.

industry, journalists warned that "[t]oday anybody with a personal computer and access to public documents can set up his own miniature private-investigating agency. Dozens of these mom-and-pop data services have sprung up, selling specialized electronic lists of police reports, arrest records, citations for motor vehicle violations, and other potentially damaging information."[131]

In *Reporters Committee*, the Court ruled that the disclosure of a compiled criminal history report—though it contained public information—constituted an invasion of privacy because it was not otherwise easily obtained.[132] The case involved the FBI's refusal to release a rap sheet to the media, citing exemption 7(C) of the Freedom of Information Act, which protects the release of information compiled for law enforcement purposes, and that releasing would be reasonably expected to constitute an unwarranted invasion of personal privacy.[133] An important component to the government's argument relied on the way criminal record information was organized and indexed in rap sheet databases (by a person's name) rather than by the organizational structure of the governmental agencies that provided the information, such as a bulk set of criminal court docket information organized by jurisdiction.[134] As Justice Stevens described, "[p]lainly there is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computer summary located in a single clearinghouse of information."[135]

Many state laws governing rap sheet privacy follow the *Reporter's Committee* precedent to limit unfettered access to criminal records, with approximately half of U.S. states treating compiled criminal histories as private information, and even among those states that treat a rap sheet as public record, only one state does so at no cost to users (thereby creating at least financial obstacles to the information).[136] These types of state-level privacy protections and accompanying administrative rules thus limit the spread of data error. For instance, in New Jersey, a person must be fingerprinted to obtain a copy of their own rap sheet (called a Computerized Criminal History, or CCH), which is maintained by the state police.[137] Third parties may access the document only with the express consent of the record subject.[138] These access limits allow for a centralized and managed set of criminal record data, organized by a subject's biometrics and state identification number.[139] Thus, when a state-produced error shows up on a CCH, a person can approach a single office to begin contesting the error. Though

[131] Philip Elmer-DeWitt, Scott Brown & Barbara Dolan, *An Electronic Assault on Privacy? Computer Blacklists Have Become a New Growth Industry*, 127 TIME 104 (1986); File, *supra* note 129, at 13–14.

[132] File, *supra* note 129, at 7.

[133] 5 U.S.C. § 552 (b)(7).

[134] File, *supra* note 129, at 17.

[135] U.S. Dep't of Just. v. Reps. Comm. for Freedom of Press, 489 U.S. 749, 764 (1989).

[136] Sandoval & Lageson, *supra* note 32, at 266.

[137] *Id.* at 272.

[138] *See id.*

[139] *NJ Criminal History Records Information: Name-Based Checks (Records from NJ Only)*, N.J. STATE POLICE, https://nj.gov/njsp/criminal-history-records/chri-nb-checks.shtml (last visited July 23, 2023) [https://perma.cc/C448-K6KG].

this often involves shifting the burden to the record subject to track down the requisite documents from court and correctional agencies to "prove" the error, the process is much more straightforward than facing hundreds, if not thousands, of versions of a person's criminal record that are housed in private sector databases.

The problem with the practical obscurity approach (and the accompanying state laws that use the case to prevent total public access to rap sheets) is that rap sheets are now but one type of criminal record information that a person may seek. While in the past, the rap sheet was considered the authoritative record, digitization has rendered the pieces of information that comprise a rap sheet incredibly easy to obtain, such as arrest records, court records, or correctional records.[140] Unlike the rap sheet, which is regulated under state administrative or penal law, arrest, court, and correctional records are maintained by different branches of government and operate under their own "patchwork"[141] of statutory, regulatory, constitutional, and common law in a "smokestack"[142] approach to data management. Thus, data error was limited by the privacy afforded through the practical obscurity doctrine—until the spread of other types of criminal record information became more easily obtainable.

Accordingly, recent critiques of practical obscurity point at the limits of relying heavily on the compilation of records argument as a way to get at criminal record privacy. Today, the compilation of governmental information into a single report is an incredibly simple task; indeed, we would simply consider this aggregated data.[143] Further, reputational and information privacy harms might actually be exacerbated by the government's unwillingness to release compiled (and arguably more accurate) criminal history information: "[i]f anything," argues Professor Jan Kirtley (the director of the Reporter's Committee organization at the time of the Court's decision), "the aggregation of disparate records over an extended period provides a more complete and contextual view of the subject's criminal history than a single document memorializing an isolated arrest at one moment in time could ever offer."[144] Plus, by focusing privacy protections to a single record (the rap sheet), the doctrine may have become, in the words of one federal judge, "an anachronism" as "[b]its and pieces of data are aggregated and immortalized on public and private systems."[145]

Practical obscurity is thus quite incompatible with the digital age. While rap sheets receive privacy protections, court, jail, and police records remain categorized as public records. In the paper age, this allowed for de facto privacy

[140] Sandoval & Lageson, *supra* note 32, at 269–70.

[141] *Id.*

[142] SEARCH GRP., INC., U.S. DEP'T OF JUST. BUREAU OF JUST. STATS., REPORT OF THE NATIONAL TASK FORCE ON PRIVACY, TECHNOLOGY, AND CRIMINAL JUSTICE INFORMATION 1 (2001).

[143] Jane E. Kirtley, *"Misguided in Principle and Unworkable in Practice": It Is Time to Discard the* Reporters Committee *Doctrine of Practical Obscurity (and Its Evil Twin, the Right to Be Forgotten)*, 20 COMMC'N L. & POL'Y 91, 92 (2015).

[144] *Id.* at 94.

[145] *Id.* at 113 (citing Am. C.L. Union v. U.S. Dep't of Just., 750 F.3d 927, 942 (D.C. Cir. 2014) (Brown, J., dissenting)).

protections. In the digital age, these records have instead become easily exportable and now constitute the foundation of private sector criminal record information. Plus, the doctrine relates only to the release of governmental information, not the regulation of information aggregated and reported by third parties—the format of the vast majority of today's criminal records.

B. Barriers Stemming from Qualified Immunity & Good Faith Exceptions

There is also very little recourse available to those who have an error on their criminal record attributable to a governmental source. This applies even if they are arrested on a faulty warrant and wrongfully incarcerated.[146] By extension, there is little incentive for the government to maintain accurate criminal record data. Exceptions and immunity derive from several areas of law but generally fall under good faith exceptions and qualified immunity.[147] What these sources of law share is shifting the burden to the harmed person to prove the error caused material damage and that the erroneous data was maintained or furnished with intent or knowledge.[148]

Suits against the individual governmental workers who are tasked with maintaining criminal record databases are most likely barred by qualified immunity unless, again, one can prove malicious intent in inserting or overlooking criminal record errors or it can be shown that a department has a "custom or policy of providing incorrect information."[149] At the state level, statutory immunity is sometimes available for data error, such as in Ohio, where a person can recover for harms caused by the errors if they can prove the state intentionally maintained information that is known or should have reasonably been known to be "inaccurate, irrelevant, no longer timely, or incomplete."[150] In Nevada, the government has qualified immunity for "transmitting or reporting an inaccurate or incomplete version of the record or taking any other required action concerning an inaccurate or incomplete version of the record,"[151] and "a qualified entity is not liable for damages solely arising out of the accuracy of any information included in or omitted from records of criminal history."[152] A broader set of statutory and case law further protects local government from errors in sex offense registries.[153]

These immunities attach to the public sector, but the private sector also receives immunity unless the complainant can prove intent: the Fair Credit Reporting Act § 1681h(e) provides qualified immunity to CRAs, users, and furnishers of information from "any action or proceeding in the nature of defamation,

[146] *See* Logan & Ferguson, *supra* note 23, at 579.

[147] *Id.* at 579–84.

[148] *Id.* at 579.

[149] *See id.* at 579–80.

[150] *See* Logan & Ferguson, *supra* note 23, at 583 (citing OHIO REV. CODE ANN. 1347.09(A)(1) (West 2022)).

[151] NEV. REV. STAT. § 179A.165 (2021).

[152] NEV. REV. STAT. § 179A.325 (2021).

[153] *See* Logan & Ferguson, *supra* note 23, at 583–84.

invasion of privacy, or negligence with respect to the reporting of information . . . except as to false information furnished with malice or willful intent to injure such consumer."[154] This is not the only limit to the Fair Credit Reporting Act, however, which is discussed below.

C. Limits to the Fair Credit Reporting Act

Most challenges to inaccurate criminal background checks are litigated through the Fair Credit Reporting Act, a federal statute originally intended to protect consumers by improving the accuracy of credit reports. It was enacted in 1970 and is enforced by the Federal Trade Commission ("FTC").[155] For people with criminal records, the FCRA creates processes for Consumer Reporting Agencies ("CRAs") to follow in an effort to produce accurate and updated background-checking information.[156] The FCRA also provides limits to the types of adverse information that show up on a background check, such as requiring CRAs to remove from their reports any arrest records from over seven years ago,[157] which can also serve to strengthen the face validity of background checks by removing non-conviction information that may reflect police bias or overzealous prosecution. Subjects of FCRA-compliant background checks are also provided an avenue to challenge incorrect information that appears on a report, and litigation has followed where CRAs have been shown to fail to follow reasonable procedures to ensure maximum accuracy.[158]

Accuracy itself is not defined by the FCRA,[159] but the Eleventh Circuit has followed dictionary definitions of accuracy, and as applied to consumer reports, "being free from 'mistake' or 'error' means being free from a 'misunderstanding of the meaning or implication of something."[160] Case law has also interpreted information that is obsolete or outdated as inaccurate, a position also supported by the FTC.[161] For some time, industry litigants relied on a "technical accuracy" defense, but this was reversed in *Twuamasi-Ankrah v. Checkr, Inc.* in 2020, where the Sixth Circuit held that a plaintiff may allege that a CRA reported *either* "patently incorrect" information or "information that was 'misleading in such a

[154] 15 U.S.C. § 1681h(e).

[155] *See generally* 15 U.S.C § 1681.

[156] Elizabeth Westrope, *Employment Discrimination on the Basis of Criminal History: Why an Anti-Discrimination Statute Is a Necessary Remedy*, 108 J. CRIM. L. & CRIMINOLOGY 367, 377–78 (2018).

[157] 15 U.S.C. § 1681c(a).

[158] Westrope, *supra* note 156, at 379.

[159] *See id.* at 142–43.

[160] *See id.* (citing Erickson v. First Advantage Background Servs. Corp., 981 F.3d 1246, 1251–52 (11th Cir. 2020) (defining "mistake" as a "misconception or misunderstanding")).

[161] *Id.* at 143 n.128 (citing FED. TRADE COMM'N, COMPLIANCE WITH THE FAIR CREDIT REPORTING ACT 28 (1977); Seamans v. Temple Univ., 744 F.3d 853, 866 (3d Cir. 2014) ("furnisher's failure to provide date of first delinquency, which triggers 7-year obsolescence period, could be considered incomplete and inaccurate reporting"); Beseke v. Equifax Info. Servs. LLC, No. 17-4971, 2022 WL 133289, at *3 (D. Minn. Jan. 13, 2020) ("misimpression as to age of delinquency remains distinct and viable claim for inaccuracy"); Clements v. Trans Union, LLC, No. 17-CV-00237, 2018 WL 4519196, at *8 (S.D. Tex. Aug. 29, 2018), *adopted*, 2018 WL 4502255 (S.D. Tex. Sept. 20, 2018) ("CRA that includes obsolete information is 'in effect, providing misleading information'")).

way and to such an extent'" to have been expected to create an adverse effect on the report subject.[162]

There is a special FCRA accuracy requirement for "adverse" public records (including arrests, indictments, and convictions) that only applies when the background check is used for employment contexts that *should* help improve the accuracy of such information.[163] CRAs have two options when providing this type of information to an employer: first, the CRA can notify the record subject that the public record information is being reported to the employer; or second, the CRA can maintain "strict procedures" to ensure the public record information is complete and up to date before furnishing the report.[164] The first option must be utilized when a CRA is subscribing to a data furnisher and accessing their private database of aggregated public records, and the notice must be sent immediately upon the CRA accessing the public record information.[165] Unfortunately, procedures tied to this requirement are antiquated: CRAs are allowed, for instance, to only send notice via first class mail even when a background check is instantly created and delivered to the requester digitally.[166] Interviews with background screening company officials have also revealed that the contemporaneous notice requirement might even disincentivize accuracy checks once notice is sent.[167]

For the second option, a CRA must ensure that the report accurately reflects the "current public record status of the item at the time of the report is reported,"[168]—and relying on a database that is updated only monthly, for instance, does not suffice.[169] This requires the CRA to maintain "strict" procedures, rather than the "reasonable procedures" accuracy standard of the FCRA more generally, and includes things like verifying the identity of the person contained in the report and accurately reporting whether a conviction was for a misdemeanor or conviction.[170] Yet, even these safeguards fail to quell the widespread problem of criminal record accuracy.

First, while the FCRA limits the disclosure of some types of criminal record information (such as those arrests that did not lead to a conviction and are from

[162] 954 F.3d 938, 942 (6th Cir. 2020).

[163] 15 U.S.C. § 1681k.

[164] *Id.*

[165] *See* Chi Chi Wu et al., Nat'l Consumer L. Ctr., Fair Credit Reporting 226–27 (10th ed. 2022).

[166] *See id.*; Taylor v. Selection Mgmt. Sys., Inc., No. 18-cv-224, 2021 WL 274445, at *8 (S.D. Ohio Jan. 27, 2021) ("Although providing consumer access to the reporting agency's system at the same time it provides access to the user may allow for 'technological symmetry,' the FCRA does not require this . . . ."); Henderson v. Trans Union, LLC, No. 14–cv–00679, 2017 WL 1734036, at *3–4 (E.D. Va. May 2, 2017) (summary judgment for consumer reporting agency holding that starting the mailing process at the time a consumer reporting agency realizes that notice may be required does not rise to reckless violation of § 1681k); Williams v. First Advantage LNS Screening Sols., Inc., 155 F. Supp. 3d 1233, 1249–1250 (N.D. Fla. 2015) (noting, but not deciding, the issue of whether a consumer reporting agency may send notice by first class mail when it sends report to employer electronically); Smith v. E-Backgroundchecks.com, Inc., 81 F. Supp. 3d 1342, 1363 (N.D. Ga. 2015) (relying on FTC Staff Summary to permit sending notice by first class mail, even though it would not be contemporaneous notice).

[167] *See* U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 22, at 38–39.

[168] 15 U.S.C. § 1681k(a)(2).

[169] *See* U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 22, at 38.

[170] *See* WU ET AL., *supra* note 165, at 227–28.

over seven years ago),[171] these types of information are widely available on the internet through "people search" and other public record aggregator services. A simple (and common) Google search for a job candidate will quickly reveal criminal records maintained by "non-FCRA" criminal record providers on the internet.

Second, employers can simply sidestep FCRA protections by simply looking up public records themselves: the FCRA does not apply to institutional decision-making processes, such as employment, if the employer, for instance, browses online court records.[172] In a report funded by the Federal Bureau of Justice Statistics in 2005, a Task Force on Criminal History Information raised the question of FCRA applicability to how criminal background checking really operates in the American public records context.[173] The report pointedly asked:

> Does it really make any sense that different privacy protections apply when the exact same information is held by different parties? Specifically, does it make sense that when commercial vendors communicate criminal history data to employers, the protections in the FCRA apply; but, when employers obtain these data directly from courts or law enforcement, and do so for the very same purpose, none of these protections apply?[174]

Third, the FCRA does not account for variations in state expungement and sealing laws, so an offense that might be sealed under state law may still appear on a CRA's background check.[175] The FCRA does not speak directly to expunged records, so an applicant may initiate the FCRA's dispute process if a sealed record wrongfully appears in a background check, but this is not always practicable or desired.[176]

Finally, the FCRA distinguishes between data "furnishers" and the CRAs that produce background check reports. Furnishers, which provide the underlying criminal record information to CRAs, are subject to a number of FCRA requirements,[177] but there is no private right of action for many of those requirements that obligates them to provide correct and updated information. The FCRA also does not always cover "people search" engines, which warehouse and resell personal data scraped from public sources.[178] These websites affirmatively claim to opt out of the FCRA by specifically warning purchasers of their background checks that the reports are not to be used for any decision-making that could

[171] 15 U.S.C. § 1681c.

[172] Michael Carlin & Ellen Frick, *Criminal Records, Collateral Consequences, and Employment: The FCRA and Title VII in Discrimination Against Persons with Criminal Records*, 12 SEATTLE J. SOC. JUST. 109, 123 (2013).

[173] U.S. Dep't of Just., The Attorney General's Report on Criminal History Background Checks 8 (2006).

[174] SEARCH GRP., INC., U.S. DEP'T OF JUST. BUREAU OF JUST. STATS., REPORT OF THE NATIONAL TASK FORCE ON THE COMMERCIAL SALE OF CRIMINAL JUSTICE INFORMATION vi (2005).

[175] Carlin & Frick, *supra* note 172, at 136.

[176] *Id.* at 137.

[177] 15 U.S.C. § 1681s–2.

[178] *What Employment Background Screening Companies Need to Know About the Fair Credit Reporting Act*, FED. TRADE COMM'N (Apr. 2016), https://www.ftc.gov/business-guidance/resources/what-employment-background-screening-companies-need-know-about-fair-credit-reporting-act [https://perma.cc/32CV-YU4B].

result in an adverse outcome for the subject of the check.[179] In 2014, Instant Checkmate settled FTC claims that the company was selling consumer data without complying with the FCRA and was prohibited by court order from "furnishing consumer reports to anyone who does not have an FCRA-defined permissible notice."[180] Since then, Instant Checkmate has continued to sell background checks and maintained a post on its "Frequently Asked Questions" page that states:

> Instant Checkmate is a public records search service, which means there are strict guidelines as to how and why our service may be used. Most importantly, we are NOT a Consumer Reporting Agency, and therefore it is prohibited to use our site for any purpose governed by the Fair Credit Reporting Act (FCRA). So before you run a search, please review Instant Checkmate's Dos and Don'ts below to make sure that your search is permitted.[181]

The site goes on to encourage background checks on neighbors, nearby sex offenders, family members, parents of your children's friends, new and old friends, and former classmates but warns users not to use the information to make hiring, credit, or housing decisions.[182] While the company tells users that their reports "are typically very accurate," the company is also not obligated to any of the accuracy standards and related causes of action under the FCRA.[183] When a user enters the website's "Criminal Records Database," a popup warns that "the information provided on this site may not be 100% accurate."[184] Yet, it's made available to paying customers. Beyond that, forced arbitration clauses on people-search websites have precluded FCRA claims against people-search websites, even when a background check subject has suffered a harm.[185]

Amidst this backdrop, criticism has mounted regarding the FCRA's limits to adequately address the harms of criminal record error. At least one court has expressed "extreme frustration" with the FCRA, noting that the provisions are

> of little value to ordinary consumers, in part due to the fact that it is hopelessly complex—the statute is drafted in hyper-technical language and includes a sufficient number of internal cross-references to make even the most dedicated legal practitioner consider a change in career. But the FCRA's substance is even more troubling than its complex form. The

[179] *See Two Data Brokers Settle FTC Charges that They Sold Consumer Data Without Complying with Protections Required Under the Fair Credit Reporting Act*, FED. TRADE COMM'N (Apr. 9, 2014), https://www.ftc.gov/news-events/news/press-releases/2014/04/two-data-brokers-settle-ftc-charges-they-sold-consumer-data-without-complying-protections-required [https://perma.cc/USV5-W62Q].

[180] *Id.*

[181] *Instant Checkmate FAQs- Frequently Asked Questions*, INSTANT CHECKMATE, https://www.instantcheckmate.com/faqs/ (last visited July 23, 2023) [https://perma.cc/8QDF-PSX4].

[182] *Id.*

[183] *See id.*; Ed Smith, *How Accurate Are Instant Checkmate Background Reports?*, INSTANT CHECKMATE (Apr. 19, 2022), https://www.instantcheckmate.com/crimewire/post/how-accurate-is-instant-checkmate/ [https://perma.cc/DK6J-XVR6].

[184] *Traffic, Criminal and Arrest Records Search*, INSTANT CHECKMATE, https://www.instantcheckmate.com/criminal-records/ (last visited July 23, 2023) [https://perma.cc/CS8Y-FFSQ].

[185] *See* Mejia v. TruthFinder, LLC, No. 22-CV-1010-CAB-AGS, 2022 WL 5236828, at *4 (S.D. Cal. Oct. 5, 2022).

> statute includes numerous provisions that limit consumers' ability to enforce its mandates either by explicitly barring private actions or by imposing such burdensome procedural requirements that no layperson could possibly be expected to comply.[186]

Plus, people with criminal records are already contending with a great deal of practical obstacles, such as navigating family dynamics, seeking employment, and establishing safe housing. As one commentator noted, "the reality of engaging in protracted litigation often presents an insurmountable hurdle for consumers seeking relief, and, even then, only after they have been injured by erroneous reports."[187] Addressing background check error, unfortunately, may fall low on the list of a person's needs.

D. Standing Issues

Challenging an inaccurate credit report or criminal background check has also become more difficult in light of the Supreme Court's 2021 decision in *TransUnion L.L.C. v Ramirez*. Prior to this decision, litigants could sue under the Fair Credit Reporting Act through statutorily defined rights.[188] As defined in 1975, in *Warth v. Seldin*, "Congress may create a statutory right or entitlement the alleged deprivation of which can confer standing to sue even where the plaintiff would have suffered no judicially cognizable injury in the absence of statute."[189] In 2021, the Court reversed course and held that standing is limited to those rights that are protected or for which there is a close historical or common-law analogue.[190] Although the FCRA creates a right to accurate information and authorizes suits as an enforcement mechanism, the Court emphasized that these rights are not protected by common law or historical precedent.[191]

The *TransUnion* case came after standing was first addressed in *Spokeo, Inc. v. Robins* in 2016.[192] Spokeo is a people-search engine that aggregates personal information and provides in-depth reports for consumers.[193] Robins alleged his Spokeo report contained several errors pertaining to his employment and family life and sued under the FCRA.[194] The Ninth Circuit held that Robins had standing to sue, but this was reversed and remanded by the Supreme Court.[195] While the Court affirmed congressional power to create rights through statute, Justice Alito, in the majority opinion, noted that standing required a "particularized" and "concrete" injury.[196] In effect, this decision created a two-part test for

[186] *See* WU ET AL., *supra* note 165, at 571–72.

[187] Weiss, *supra* note 82, at 275.

[188] *See* Warth v. Seldin, 422 U.S. 490, 514 (1975).

[189] *Id.*

[190] Erwin Chemerinsky, *What's Standing After* Transunion LLC v. Ramirez, 96 N.Y.U. L. REV. ONLINE 269, 270 (2021).

[191] *Id.*

[192] *See* 578 U.S. 330, 333 (2016).

[193] *Id.*

[194] *See id.* at 336.

[195] *Id*. at 342–43.

[196] *Id.* at 339.

the first time.[197] Standing would now require a concrete harm; a de facto harm that is "real."[198]

Defining what constitutes a concrete harm became the basis of *TransUnion*, where a credit reporting company began to offer an add-on product called OFAC Name Screen Alert to its existing credit reporting services.[199] The product would search for people's names against a list maintained by the U.S. Department of Treasury's Office of Foreign Assets Control ("OFAC"), which contained terrorists, drug traffickers, and other serious criminals.[200] If a name matched, TransUnion would flag the person's report as a "potential" match to an OFAC name.[201] Ramirez was denied an automobile sale after a car dealer used TransUnion to run a check on Ramirez and was alerted to a potential OFAC match.[202]

A class action lawsuit followed on behalf of the 8,185 people who were flagged as potential OFAC matches.[203] The class alleged that TransUnion failed to follow reasonable procedures to ensure accuracy, as required by the Fair Credit Reporting Act, that the inaccuracies caused reputational harm, and that mailings sent by TransUnion to class members were defective.[204] The class also fell into two groups: those whose OFAC alerts were provided to third parties (such as the car dealership) and those whose erroneous records were *not* yet disseminated to any third parties.[205] In a 5-4 decision, the Supreme Court ruled that this second group, whose reports were not yet disseminated, lacked standing to sue by failing to suffer a concrete harm.[206] As legal scholar Erwin Chemerinsky summarized: "[i]n other words, even though the Fair Credit Reporting Act created a right and that right was infringed, that was not sufficient for standing."[207]

Thus, the experience of having an inaccurate criminal record tied to one's name in a private database is not itself a harm. This creates even less incentive for accuracy in the aggregation and compilation stages of creating data profiles, particularly for the data brokers who simply sell aggregate data to companies covered under the FCRA.

E. Limits to Private Enforcement

Private rights of action are difficult to leverage against governments, CRAs, and data furnishers. When the government's information is incorrect, the harmed person must show that the data error was the result of "deliberate,

[197] Chemerinsky, *supra* note 190, at 278.
[198] *Spokeo*, 578 U.S. at 340.
[199] TransUnion LLC v. Ramirez, 141 S. Ct. 2190, 2197 (2021).
[200] *Id.*
[201] *Id.*
[202] *Id*. at 2201.
[203] *Id*. at 2197.
[204] *Id.*
[205] *Id.*
[206] *Id*. at 2212.
[207] Chemerinsky, *supra* note 190, at 281.

reckless, or grossly negligent conduct" or, in some circumstances, "recurring or systemic negligence" to leverage state data privacy laws.[208]

State consumer data law also offers little recourse for people who have suffered harm due to an incorrect private-sector criminal background check. State defamation claims related to inaccurate criminal records are broadly preempted by the Fair Credit Reporting Act[209] and the tort doctrine of qualified privilege,[210] except for false information furnished with malice or willful intent to injure. As summarized by the NCLC, "[t]he qualified immunity doctrine is premised on the policy that the free flow of credit information is more important than individual claims of personal injury, and on the fear that, absent some protection from defamation liability, CRAs would not provide valuable information."[211] The Fair Credit Reporting Act further reduces states' ability to regulate consumer reporting through Section 1681t(b)(1),[212] though recent statutory interpretations by the CFPB (discussed in Part V) may be eroding some of these CRA protections.

Defamation claims against data furnishers are also preempted by the FCRA; there is no private right of action against a data furnisher that fails to withhold inaccurate data from a consumer reporting agency, even if that data furnisher knows or has been notified by a consumer that their data are incorrect.[213] The National Consumer Law Center notes that one exception applies: where a subject of a background check disputes inaccurate information with the CRA, the CRA asks the data furnisher to reinvestigate, and the furnisher fails to do so.[214] Courts, however, have misinterpreted this statute to apply only to CRAs' ability to privately enforce furnishers' failures.[215] Practically speaking, this is a burdensome and convoluted process that will be very difficult for a background check subject to pursue.

Some state laws allow recourse when data aggregators and people-search websites that proactively claim to operate *outside* of the Fair Credit Reporting Act report inaccurate criminal records. Typically, these claims fall under publicity and data privacy laws.[216] Several Illinois cases illustrate the publicity context: a third party purchases or scrapes public record information, reposts it online, and then advertises a subscription or membership based on a small tidbit of search results for a person. In a case from August 2022, *Gaul v. Truth Now LLC*, a website called InmatesSearcher showed a "free preview" of people contained in their database.[217] The plaintiff alleged that displaying her identity violated the

[208] Herring v. United States, 555 U.S. 135, 144 (2009).

[209] *See* Womble Bond Dickinson & D. Scott Anderson, *State Law Claims Beware: When FCRA Preempts Claims Brought Under Other Laws*, JD SUPRA (Oct. 18, 2018), https://www.jdsupra.com/legalnews/state-law-claims-beware-when-fcra-71954/ [https://perma.cc/23ZD-76AB].

[210] WU ET AL., *supra* note 165, at 590–92.

[211] *Id.*

[212] 15 U.S.C. § 1681t(b)(1).

[213] 15 U.S.C. § 1681s-2(a)(1)(B); *see also* WU ET AL., *supra* note 165, at 571–72.

[214] WU ET AL., *supra* note 165, at 572–73.

[215] *Id.*

[216] MINN. STAT. ANN. § 332.70 (West 2014).

[217] Gaul v. Truth Now, LLC, No. 21-CV-1314-JES-JEH, 2022 WL 3647257, at *1 (C.D. Ill. Aug. 24, 2022).

Illinois Right of Publicity Act ("IPRA"), which prohibits the use of an "individual's identity for commercial purposes" without their consent.[218] The defendants claimed CDA 230 immunity, the First Amendment, jurisdiction, and IPRA exemptions in their motion to dismiss.[219] The court found that the Plaintiff successfully pleaded that her identity was used for a commercial purpose, following another recent Illinois case against Whitepages.com and Instant Checkmate where data aggregators scraped public records (including criminal records), reposted them online, and showed a preview to advertise monthly subscription services.[220]

These limited remedies, however, require plaintiffs to show that the company used their likeness for financial gain.[221] For most people, the inaccurate or misleading information may not be advertised or even noticed until after a harm has occurred.

F. Section 230 Immunity from Suit

While Consumer Reporting Agencies must comply with the provisions of the FCRA or face potential liability, data furnishers and vendors, at times, position themselves as outside the purview of the FCRA and seek Section 230 immunity.

Broadly put, 47 U.S.C. § 230 "says that websites and other online services aren't liable for third-party content."[222] Public records aggregators that rely on governments and courts to supply the criminal record information are incentivized by Section 230 immunity to claim that any errors are attributable to the governmental source—the "third party." This was the argument in the case that opened this Article, *Henderson v. The Source for Public Data*.[223] In front of the Fourth Circuit, lawyers for the company argued that their website, which allows people to pay for criminal records, was a "simple conduit" between governmental records and the general public—and warned that regulating data brokers would be "truly dangerous to the internet."[224] Likening this case to broader debates over Section 230, the plaintiffs argued:

[218] *Id.* (quoting 765 ILL. COMP. STAT. ANN. 1075/30(a) (West 2005)).

[219] *Id.*

[220] *See* Lukis v. Whitepages Inc., 542 F. Supp. 3d 831, 835, 836, 843 (N.D. Ill. 2020).

[221] *See id.* at 837–38 (citing 765 ILL. COMP. STAT. ANN. 1075/30a (West 2005)).

[222] Eric Goldman, *An Overview of the United States' Section 230 Internet Immunity*, *in* THE OXFORD HANDBOOK OF ONLINE INTERMEDIARY LIABILITY 155 (Giancarlo Frosio ed., 2020).

[223] *See* Brief of Defendants-Appellees at 16, Henderson v. Source for Pub. Data, L.P., 53 F.4th 110 (4th Cir. 2022) (No. 21-1678), 2022 WL 103151, at *16.

[224] Jon Hill, *4th Circ. Is Warned of Internet 'Open Season' in FCRA Appeal*, LAW360 (May 3, 2022, 10:37 PM), https://www.law360.com/articles/1489651/4th-circ-is-warned-of-internet-open-season-in-fcra-appeal [https://perma.cc/8V3H-XC2Z].

> We see the hostility towards Facebook, Twitter that's out there in the political sphere. If this kind of loaded gun can be out there, that you can put any regulation on an interactive computer service you want, as long as you don't change the content of what they're posting . . . then it's open season.[225]

Public Data was relying on several decades of Section 230 cases where websites only lose immunity if they "materially contribute" to posted content—not simply compiling and reposting content taken from a different source.[226] This has included false or defamatory material "so long as the information was provided by another party."[227] As applied to Henderson and the others in the class who had inaccurate criminal records posted to the Public Data website, the company argued that Public Data merely retrieves and transmits public court records obtained directly from government entities and displays results responsive to the query submitted without further evaluation, commentary, or material contribution/alteration.[228]

The *Henderson* case specifically bridges FCRA and 230: the company was granted CDA 230 protection for four FCRA violation claims in District Court.[229] In November 2022, the Fourth Circuit Court of Appeals reversed and remanded.[230] "Section 230(c)(1) of the Communications Decency Act protects some parties operating online from specific claims that would lead to liability for conduct done offline," stated the court, "[b]ut it is not a license to do whatever one wants online."[231]

The *Henderson* case might be just the start. Courts are increasingly skeptical that people search and public records aggregators are doing nothing more than merely hosting user-generated content and are instead "actively tak[ing] content from other sources," curating it, and uploading it to a website in a "novel configuration for repurposed uses."[232] Ongoing, potentially "precedent setting cases"[233] are moving through the courts after surviving motions to dismiss, including *Cat Brooks et al v. Thomson Reuters*, a class action lawsuit against Thompson Reuters' CLEAR Reports, which the company argues "is simply a

[225] *Id.*

[226] *See* Brief of Defendants-Appellees, *supra* note 223, at 13, 28–29 (citing Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157, 1162–63 (9th Cir. 2008)); *id.* at 39–40 (citing Prickett v. infoUSA, Inc., 561 F. Supp. 2d 646, 649, 652 (E.D. Tex. 2006)).

[227] Carafano v. Metrosplash.com, Inc., 339 F.3d 1119, 1122 (9th Cir. 2003).

[228] *See* Brief of Defendants-Appellees, *supra* note 223, at 13.

[229] Henderson v. Source for Pub. Data, 540 F. Supp. 3d 539, 549 (E.D. Va. 2021), *rev'd*, 53 F.4th 110 (4th Cir. 2022).

[230] *Henderson*, 53 F.4th at 129–30.

[231] *Id.* at 117.

[232] Eric Goldman, *Three More Yearbook/People Database Cases Signal Trouble for Defendants*, TECH. & MKTG. L. BLOG (May 18, 2022), https://blog.ericgoldman.org/archives/2022/05/three-more-yearbook-people-database-cases-signal-trouble-for-defendants.htm [https://perma.cc/CR55-ABWB] (citing Kellman v. Spokeo, Inc., 599 F. Supp. 3d 877, 898 (N.D. Cal. 2022)).

[233] Lyell Marks, *Right to be Forgotten—Precedent Setting Cases Have Begun (CAT BROOKS et. al. v. THOMSON REUTERS CORPORATION)*, W. INTEGRATED SYS. (Oct. 1, 2021), https://www.westint.com/right-to-be-forgotten-precedent-setting-cases-have-begun-cat-brooks-et-al-v-thomson-reuters-corporation/ [https://perma.cc/JJ6G-Y9P5].

compilation of public records" but are sold to private companies, law enforcement, investigative firms, and ICE.[234] While this case focuses on the profiteering and privacy-violating practices of CLEAR, accuracy problems are also part of the alleged harms perpetuated by the company.[235]

Though an increasingly politicized legal doctrine, these shifting views of Section 230 protection may offer those harmed by inaccurate criminal records a small step towards more accurate and more fair reporting of their criminal histories by being able to leverage the Fair Credit Reporting Act in a digital environment. While privacy claims are yet to be realized under 230, accuracy claims are becoming more viable.

But we need bigger and more fundamental reform to protect both subjects and users of criminal records. The following Part proposes several options.

V. SOLUTIONS

The American exceptionalism of using criminal records in nearly all facets of institutional life relies on a very shaky premise: that criminal record information is accurate enough to be of use at all. People who are harmed by inaccurate criminal records—and even those who have yet to be harmed but are unaware of the state of their criminal record information—have very little legal protection. Any recourse relies on a person identifying error, experiencing a harm, proving malice or willful neglect, and scraping together the time, resources, and experts needed to prove their harm. Even then, the harmed criminal record subject can hope only for modest monetary damages or a settlement—which does nothing to remedy the errors likely contained in innumerable other databases. Companies who deal in criminal record data continue to broker, aggregate, and share data in an essentially unregulated manner with little concern toward accuracy.

Governmental error is exacerbated by a lack of centralized data and centralized goals. Federal committees and government-funded reports have long recognized the need to improve criminal justice data but have provided little guiding standards or consistent resources to do so.[236] The impetus for much of the work has also been to improve criminal records for law enforcement and investigatory purposes—not for regulating the flow of data into the private sector to promote accuracy.[237] The local and siloed nature of criminal justice data (and particularly the sale of bulk criminal court data) has persistently undercut these

[234] *Id.*

[235] *See* First Amended Class Action Complaint at 11, Brooks v. Thomson Reuters Co., No. 3:21-cv-01418-EMC, 2021 BL 308667 (N.D. Cal. Feb. 26, 2021).

[236] *See* Genesis Guzman, *Inadequate Data Collection Is Slowing Down Criminal Justice Reform*, DAVIS VANGUARD (Aug. 18, 2021), https://www.davisvanguard.org/2021/08/inadequate-data-collection-is-slowing-down-criminal-justice-reform/ [https://perma.cc/HS8B-UBYG].

[237] *See* Palmer Gibbs, *The Benefits of Data in Criminal Justice: Improving Policing*, SUNLIGHT FOUND. (Apr. 29, 2015, 4:44 PM), https://sunlightfoundation.com/2015/04/29/the-benefits-of-data-in-criminal-justice-improving-policing/ [https://perma.cc/9BLT-CY94].

recommendations, while the private sector has dramatically expanded data integrity problems.

We need a new set of incentives that will promote data accuracy. This Article concludes by arguing states need to rein in their criminal justice data as a valuable resource in a data-rich economy nested within a society that, for better or worse, both values and routinely uses criminal record data. Protecting criminal record data at the state level will help deflate private sector dominance and allow people to zero in on a single source of criminal record error. The following set of potential solutions span from technical and policy-oriented (such as reorganizing state data, regulating end users, and expanding consumer protection and data privacy law) to social-structural (by recognizing the inherent harms of the systems that create criminal record data to communities of color). In general, these solutions share the orientation that criminal records ought to be considered a form of aggregated, personal data that fuels algorithmic and automated decision-making, even when rooted in inaccurate, outdated, and unfair information.

A. Centralize, Regulate, and Monetize State Data for End Users

A major contribution to criminal record error occurs because different agencies and jurisdictions, even within the same state, distribute different types of criminal record information with varying degrees of identifiers and details. For example, in New York, the state Division of Criminal Justice Services maintains New York State Criminal History Records (what this agency calls "official criminal history records"), a fingerprint-based rap sheet that includes all arrests, indictments, convictions, and sentence information from agencies across the state.[238] The DCJS website also notes that "[t]hese records are not considered public records. They cannot be provided under the state's Freedom of Information Law and DCJS does not release criminal history records to third parties or businesses that sell 'background checks.'"[239] For an in-state resident, the cost is $13.50, and for an out-of-state resident it is $43.50.[240] The records can only be requested by the subject of the record or an employer seeking the record under a local, state, or federal law.[241] The New York State Office of Court Administration ("OCA"), however, also provides a "New York Statewide criminal history record search" for $95, which is based only on name and date of birth, rather than fingerprints.[242] The court website states several times that cases may contain missing dispositions and that the results are not "certified," but anyone is allowed

[238] *Requesting Your New York State Criminal History*, N.Y. STATE: DIV. CRIM. JUST. SERVS., https://www.criminaljustice.ny.gov/ojis/recordreview.htm (last visited July 23, 2023) [https://perma.cc/FU92-4U5Y].

[239] *Id.*

[240] *Id.* (information found by selecting the "Requesting Your Criminal History while Living in New York State" and "Requesting Your Criminal History while Living Outside of New York State").

[241] *Id.*; *Criminal History Record FAQs*, N.Y. STATE: DIV. OF CRIM. JUST. SERVS., https://www.criminaljustice.ny.gov/ojis/documents/FAQs-CHRI-Access.pdf (last visited July 23, 2023) [https://perma.cc/MFC2-UTCK].

[242] *Criminal History Record Search: Overview*, NYCOURTS.GOV, http://ww2.nycourts.gov/apps/chrs/index.shtml (last visited July 23, 2023) [https://perma.cc/38E7-BBJT].

to request another person's record—even though it is likely less accurate than the rap sheet maintained by DCJS.[243]

A simple first step in reducing error would be for state governments to sweep all criminal record data disclosures linked to a person's name under their existing policy for compiled criminal histories. Approximately 50% of states consider these records private, and those states that make the records available typically only release criminal convictions for a set period of time.[244] To avoid conflicts with existing state transparency and public records laws governing police and court data, states could transfer authority to release criminal record bulk data via data-sharing agreements with registered vendors, members of the public, or researchers. Arrest and court records could remain available for public viewing at the chronologically-ordered *case* level rather than at the bulk data or person level, adopting a digital practical obscurity approach. States and counties should also refrain from actively producing digital criminal record data on their websites that can be scraped by third parties and instead adopt simple web-scraping protections, such as for historical jailhouse rosters.[245]

To fund these efforts, states can simply monetize subscription-based access to their criminal record repositories, relying on existing fee structures for person-level searches of the rap sheet database. A one-stop shop for criminal records at the state level would improve data quality within states, across states for FBI checks, and in the private sector. Rising data acquisition costs and subscription agreements would, in turn, reduce the market for cheap and inaccurate third-party vendors and incentivize more transparent uses of data.

B. Provide No-Cost Access to Data Subjects

The FCRA is not a strict liability statute and instead relies on a harmed person to pursue a claim.[246] This is not a viable option for most people harmed by bad criminal record data.[247] A better alternative would be to help prevent error by offering data transparency to subjects of criminal records by ensuring they can access and review their record. This applies to both governmental and private sector contexts. In many states, people must pay a cost to access their own state rap sheet.[248] It is not yet clear whether criminal and public record information is a required part of the Fair Credit Reporting Act's duty imposed on CRAs to provide people with an annual disclosure of their credit report from the major credit reporting agencies—but it could be mandated.[249] Search websites should also

[243] *Id.*

[244] *Id.* at 261 tbl.1.

[245] *Web Scraping Protection: How to Prevent Scraping & Crawler Bots*, DATADOME (Nov. 7, 2022), https://datadome.co/learning-center/scraper-crawler-bots-how-to-protect-your-website-against-intensive-scraping/ [https://perma.cc/2Q3L-KZZK].

[246] *See* 15 U.S.C. § 1681i(a)(1)(A).

[247] Weiss, *supra* note 82, at 275.

[248] *See Identity History Summary Checks (Rap Sheets)*, FBI, https://www.fbi.gov/how-we-can-help-you/more-fbi-services-and-information/identity-history-summary-checks (last visited July 23, 2023) [https://perma.cc/6V8Q-3WNG].

[249] *See infra* text accompanying notes 253–54.

provide no-cost reviews of one's own record alongside clear opportunities to opt out of the publicly accessible database with a single click.

Economists have long posited that providing *more* information about criminal records might serve more just ends.[250] Rather than expanding policies that aim to conceal criminal records but are nearly impossible to enforce in a digital environment (such as expungement or Ban the Box), more access to information by data subjects might lead to more fair uses of information—and, by extension, more accurate information.

The credit-scoring industry has embraced this approach. Credit card companies and third parties like *Credit Karma* offer continual credit monitoring services that provide updated credit score information, account information, and identity theft monitoring.[251] These same principles could be applied to developing criminal record monitoring, where CRAs are obligated to provide people with instant access to their criminal record or background check information, or at least at the same speed by which the companies are able to supply such information to paying customers.

At the very least, people should have access to their criminal histories in the same manner they are allowed access to their medical records, credit scores, and educational transcripts. These are all administrative documents that can dramatically shape life outcomes. Because criminal records are offered by both the public and private sectors, people should have a right to access from both sources, at no cost, and as often as they'd like.

C. Expand State Consumer Protection and Data Privacy Laws

Despite its faults, the FCRA has significant potential to remedy criminal record error in the age of big data. Perhaps recognizing the power of the FCRA, the CFPB recently issued an interpretation that aims to reduce errors in background-checking; made effective November 10, 2021, the CFPB indicated that using name-only matching procedures is a violation of Section 607(b) of the FCRA, which requires a company to use reasonable procedures to assure maximum possible accuracy.[252] This interpretation may open the door for plaintiffs to go after CRAs that use this approach, particularly smaller companies that use sloppy techniques to cut costs.

In line with very recent trends,[253] courts should continue to deny Section 230 protection to background check companies who claim to be innocent aggregators of public data that rely on third-party content. Just because a company affirmatively claims to be outside the purview of FCRA and deserving of 230

[250] *See generally* Lior Jacob Strahilevitz, *Privacy Versus Antidiscrimination*, 75 U. CHI. L. REV. 363 (2008).

[251] Alexandria White, *The Best Credit Monitoring Services That Can Help You Spot Fraud Early*, CNBC (Mar. 1, 2023), https://www.cnbc.com/select/best-credit-monitoring-services/ [https://perma.cc/3KEL-ZFEL].

[252] Fair Credit Reporting; Name-Only Matching Procedures, 86 Fed. Reg. 62, 468 (Nov. 10, 2021) (to be codified at 12 C.F.R. pt. 1022).

[253] *See generally* Brooks v. Thomson Reuters Corp., No. 21-CV-01418-EMC, 2021 WL 3621837 (N.D. Cal. Aug. 16, 2021).

immunity does not mean that company is not in the business of profiting from background checks used to justify employment and housing discrimination. Put simply, companies that create dossiers of information on people and sell or share that information to other users should be regulated under the Fair Credit Reporting Act or relevant state consumer data law.

Increasing the remedies available to people harmed by bad data might offer a stronger incentive. Right now, states face a relatively paltry fine of $31,980[254] for failing to maintain complete and accurate criminal history records (though this does not apply to police or court data arranged chronologically and intended as a public record).[255] This could obviously be increased. Statutory damages to a CRA under the FCRA range from $100 to $1,000, which could also be increased.[256] Courts could also allow a cause of action against a state or local criminal justice agency for failing to update incorrect criminal record information.[257]

States can better protect residents from the harms of inaccurate criminal records through data privacy laws. Another recent CFPB interpretation clarifies that states are not preempted from creating laws that forbid consumer reporting agencies from including arrest records in a consumer report.[258] The rule also applies to data furnishers.[259] According to the Bureau, the portions of the FCRA that are concerned with arrests and other forms of public records (like tax liens and eviction records) only regulate the length of time such information can be shared on a report—and, crucially—not the disclosure of the content itself.[260] Thus, a state could write a law that bars data furnishers and background check companies from reporting arrests at all.[261] As the NCLC summarizes, the FCRA's preemption rule might be best conceptualized as a floor rather than a ceiling.[262]

Plaintiffs may have other options to explore. State Unfair and Deceptive Business Practices ("UDAP") statutes are also a possible avenue for the harms

[254] 28 C.F.R. § 85.5 (2023).

[255] 28 C.F.R. § 20.20 (2023).

[256] 15 U.S.C. § 1681n.

[257] Logan & Ferguson, *supra* note 23, at 604.

[258] The Fair Credit Reporting Act's Limited Preemption of State Laws, 87 Fed. Reg. 41,042, 41,042 (July 11, 2022) (to be codified at 12 C.F.R. pt. 1022).

[259] *Id.* ("States therefore retain substantial flexibility to pass laws involving consumer reporting to reflect emerging problems affecting their local economies and citizens. For example, if a State law were to forbid consumer reporting agencies from including information about medical debt, evictions, arrest records, or rental arrears in a consumer report (or from including such information for a certain period of time), such a law would generally not be preempted. Likewise, if a State law were to prohibit furnishers from furnishing such information to consumer reporting agencies, such a law would also not generally be preempted.").

[260] *Id.* at 41,045–46.

[261] *See id.* ("Section 1681t(b)(1) preempts only State laws concerning the subject matter regulated under the specified FCRA sections, and whether or when information such as eviction information, rental arrears, or arrest records appears on a consumer report is not such a subject matter.").

[262] *See* WU ET AL., *supra* note 165, at 593–94; *see also* 15 U.S.C. § 1681t(a) ("Except as provided in subsections (b) and (c), this title does not annul, alter, affect, or exempt any person subject to the provisions of this title from complying with the laws of any State with respect to the collection, distribution, or use of any information on consumers or for the prevention or mitigation of identity theft, except to the extent that those laws are inconsistent with any provision of this title, and then only to the extent of the inconsistency.").

wrought by an inaccurate criminal record.[263] States are also beginning to recognize their role in regulating data brokers, including California, Nevada, and Vermont.[264] Recently proposed legislation in Pennsylvania, for instance, establishes "a data broker registration within the Office of Attorney General. Under the bill, data brokers who collect information on Pennsylvanians would be required to annually register with the Attorney General and provide information to consumers on how they may opt out of the sale of their personal information."[265]

Pennsylvania is also a national leader in the Clean Slate movement, which aims to automate the bulk sealing of certain criminal records after a prescribed time since the offense[266] and has already automatically sealed over 40 million criminal records from public view.[267] Paired with the Clean Slate legislation also came new limits on the sale and distribution of bulk court data, with requirements that subscribers to the centralized court database refresh their data weekly as new bulk record-sealing orders are implemented, [268] a "LifeCycle file" approach that helps prevent the reporting of expunged records.[269] When third parties enter into subscription agreements with the Pennsylvania court system, they must agree to regularly retrieve updated lists of newly expunged cases and update their internal criminal records systems.[270] The subscriber must also agree to allow the state court system to audit their private database.[271]

Other states have developed consumer privacy rights in ways that, if expanded or reinterpreted, could improve criminal record accuracy in the private sector. The California Consumer Privacy Act (CCPA), for instance, mandates that companies disclose personal information collected about a resident, including the right to know, delete, and opt-out of data collection,[272] but exempts publicly available information that has been disclosed by local, state, or federal

[263] *See generally, e.g.*, Lauren Stewart, Note, *Big Data Discrimination: Maintaining Protection of Individual Privacy Without Disincentivizing Businesses' Use of Biometric Data to Enhance Security*, 60 B.C. L. REV. 349 (2019).

[264] *See State Laws Related to Digital Privacy*, NAT'L CONF. STATE LEGISLATURES (June 7, 2022), https://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx [https://perma.cc/BZ9T-3Y7Z].

[265] Memorandum from Representative Frank Burns on Pennsylvanians' Online Pers. Data to All House Members (June 21, 2022, 3:50 PM), https://www.legis.state.pa.us//cfdocs/Legis/CSM/showMemoPublic.cfm?chamber=H&SPick=20210&cosponId=37520 [https://perma.cc/RM89-QN2N].

[266] *See Clean Slate: Changing Lives with Innovative Record Clearing*, MY CLEAN SLATE PA (Apr. 7, 2022), https://mycleanslatepa.com/#:~:text=To%20date%2C%20over%201.2%20million,million%20cases%20have%20been%20sealed [https://perma.cc/7VP6-DZ8N].

[267] *Id.*

[268] *See Agreement Concerning Bulk Distribution of Electronic Case Record Information on Recurring Basis*, NAT'L EMP. L. PROJECT, https://www.nelp.org/wp-content/uploads/PA-Courts-Agreement-Distribution-Electronic-Case-Record-Information.pdf [https://perma.cc/UUW7-XJJY].

[269] CONSUMER FIN. PROT. BUREAU, MARKET SNAPSHOT: BACKGROUND SCREENING REPORTS 16–17 (2019), https://files.consumerfinance.gov/f/documents/201909_cfpb_market-snapshot-background-screening_report.pdf [https://perma.cc/67T3-XYN2].

[270] NELSON, *supra* note 20, at 23.

[271] CONSUMER FIN. PROT. BUREAU, *supra* note 269, at 16.

[272] *See California Consumer Privacy Act (CCPA)*, CAL. DEP'T OF JUST. (Feb. 15, 2023), https://oag.ca.gov/privacy/ccpa [https://perma.cc/FJW5-6WRK].

governments from mandated disclosure to the data subject.[273] This means that inaccurate criminal record data will remain unmonitored by data subjects even as it is furnished to people search websites and background check companies.

This is not necessarily a barrier, though applying these expanding state-level consumer protections to privately held criminal record data will require a shift in how we characterize bulk public records data: though originating in public sources, transformed by aggregation into a new data product that should be regulated under a consumer privacy regime. The practical obscurity doctrine may play a central role in understanding how data aggregation changes the nature of purportedly "public" records.[274] As the Ninth Circuit recently noted in *Brooks v. Thomsen Reuters,* the compilation of even public records information changes its character in a fundamental way,[275] citing a 1994 public records case regarding addresses in that "[a]n individual's interest in controlling the dissemination of information regarding personal matters does not dissolve simply because that information may be available to the public in some form."[276]

D. Reframe as Racial and Algorithmic Injustice Issue

Given the ubiquity of background checking in America, it is quite obvious that the information contained therein should be as objective, transparent, and fair as possible. [277] The problem, however, is that the institutions contributing the data that eventually becomes a background check are not objective, transparent, or fair institutions. Instead, criminal justice, housing, and finance systems have a long history of racial discrimination that has created the conditions for racially biased background and credit checks today.[278] The veneer of objectivity of a background check, moreover, glosses over these racialized histories by purporting to offer a fair assessment of a person's riskiness or trustworthiness. When these reports are based on faulty information, the system fails even more.

It's plain that race structures criminal legal system operations. Decades of statistical evidence show bias in every stage of the criminal proceedings—including police discretion, charging decisions, and case outcomes.[279] But social science research has also documented racialized patterns to criminal record *error*: David McElhattan's recent study of state criminal record systems used

[273] Assemb. Bill 1355, 2019 Leg., Reg. Sess. (Cal. 2019).

[274] Hartzog & Selinger, *supra* note 126, at 1356.

[275] Brooks v. Thomson Reuters Corp., No. 21-CV-01418-EMC, 2021 WL 3621837, at *9 (N.D. Cal. Aug. 16, 2021).

[276] U.S. Dep't of Def. v. Fed. Lab. Rels. Auth., 510 U.S. 487, 500 (1994).

[277] *See, e.g.*, *Tenant Screening with Criminal Background Checks: Predictions and Perceptions Are Not Causality*, HUD (May 17, 2022), https://www.huduser.gov/portal/pdredge/pdr-edge-frm-asst-sec-051722.html [https://perma.cc/FB9R-MNAH].

[278] *See* Sarah Esther Lageson, Opinion, *How Criminal Background Checks Lead to Discrimination Against Millions of Americans*, WASH. POST (July 10, 2020, 4:35 PM), https://www.washingtonpost.com/opinions/2020/07/10/personal-data-industry-is-complicit-bad-policing-it-must-be-held-accountable/ [https://perma.cc/X92A-AC7N].

[279] Joan Petersilia, *Racial Disparities in the Criminal Justice System: A Summary*, 31 CRIME & DELINQ. 15, 15 (1985).

multivariate analyses to show that states where Black people make up a larger share of felony-record populations also have the most faulty criminal record data systems (measured by missing case dispositions), and yet legally mandate criminal background checks even though the data quality is low.[280] As he describes it, the analysis carries "implications for understanding the racialized burdens of a criminal record, as well as broader processes in the development of the American penal state that combine harsh formal punishments with chronic administrative neglect."[281]

The purportedly objective nature of a criminal record has a "tendency to abstract away critical social and historical contexts and minimize the structural conditions that underpin problems of algorithmic unfairness."[282] Even when race is deliberately removed from an algorithmically derived score or automated decision-making, the structure of racial categorization in the United States structures other inputs, such as criminal history, financial status, consumer behavior, property value, and lines of credit.[283]

The function creep of the criminal legal system into algorithmic governance can be partly explained away by the public availability of criminal justice system and criminal court data in the digital age, creating a deep trove of personal data that can be scraped and aggregated by data brokers at very little cost. It is worth considering the broader neoliberal, racial project at play here too, though. Sociologist David Garland describes in *The Culture of Control* how crime control policy emerged as a cultural-political response to changing social and demographic conditions, and one key outcome is the emergence of public-private partnerships aimed at the commercialization of crime control and the expansion of criminal records into all facets of American life.[284] As he argues,

> [t]his embrace of the private sector is liable to have fateful consequences, as it begins to transform the character of the crime control field, setting up new interests and incentives, creating new inequalities of access and provision, and facilitating a process of penal and security expansion that might otherwise have been more constrained.[285]

In this vein, the ubiquity and public disclosure of criminal records are also a strongly American phenomenon. In Europe, for instance, criminal records are widely considered a private source of information and are further restricted to encourage rehabilitation and prevent recidivism.[286] The American criminal legal

[280] *See* McElhattan, *supra* note 94, at 367.

[281] *Id.*

[282] *See* Alex Hanna, Emily Denton, Andrew Smart & Jamila Smith-Loud, *Towards a Critical Race Methodology in Algorithmic Fairness*, 2020 CONF. ON FAIRNESS, ACCOUNTABILITY, & TRANSPARENCY 501, 501 (2020).

[283] *See* Michelle Singletary, *Credit Scores Are Supposed to Be Race-Neutral. That's Impossible.*, WASH. POST (Oct. 16, 2020), https://www.washingtonpost.com/business/2020/10/16/how-race-affects-your-credit-score/ [https://perma.cc/4JJE-VLTJ].

[284] DAVID GARLAND, THE CULTURE OF CONTROL: CRIME AND SOCIAL ORDER IN CONTEMPORARY SOCIETY 117 (2001).

[285] *Id.*

[286] *See* James B. Jacobs & Elena Larrauri, *Are Criminal Convictions a Public Matter? The USA and Spain*, 14 PUNISHMENT & SOC'Y 3, 4 (2012). *But see* Alessandro Corda, Marti Rovira & Andrew Henley, *Collateral*

system, already marked by mass incarceration and mass criminalization at rates far beyond other wealthy countries, further expands the carceral state by institutionalizing criminal records into everyday life. Lacking federal internet privacy safeguards, such as Europe's GDPR and Right to Be Forgotten, the American digital landscape infuses criminal record stigma into social and digital life as well.

The repackaging of criminal record information as objective and truthful thus masks its often racist origins and faulty data quality while simultaneously legitimizing its own existence. As criminal records continue to operate as part of a broader algorithmic governance, urgent questions must be asked about the efficacy and fairness of such data that could bring creative and equitable solutions. Critical race scholarship on data surveillance has invoked the idea of reparative algorithms that "name, unmask, and undo allocative and representational harms as they materialize in sociotechnical form."[287] Activism around tying algorithmic injustice to reparations is also growing outside academia; for instance, the California Reparations Task Force, established in 2020,[288] directly confronted algorithmic opacity and technological discrimination in a 2022 meeting.[289] The organization Data for Black Lives (D4BL) has been instrumental in tying computing, big data, and algorithms into conversations and actions around oppression and injustice.[290] D4BL recently launched its #NoMoreDataWeapons initiative that fights against technologies that surveil, police, and criminalize Black and Brown communities.[291] Ruha Benjamin, a leading scholar and activist on race and technology, has introduced the concept of the "New Jim Code" to describe how algorithmic approaches can "hide, speed, and even deepen discrimination, while appearing neutral and even benevolent when compared to racist practices of a previous era."[292]

Automated decision-making and algorithmic governance thus rely on bad data in multiple ways: through factual errors in data, through unfair and racially biased data collection and labeling, through administrative neglect in updating or remedying error, and through creating structural barriers to accessing remedies for the harms caused by such data. It's time to rethink the way we use criminal records.

Consequences of Criminal Records From the Other Side of the Pond: How Exceptional is American Penal Exceptionalism?, CRIMINOLOGY & CRIM. JUST. 1, 9 (2023).

[287] Jenny L. Davis, Apryl Williams & Michael W. Yang, *Algorithmic Reparation*, 2 BIG DATA & SOC'Y 1, 1 (2021).

[288] *See* Assemb. B. 3121 (CA 2020).

[289] Lakshmi Sarah, *From Credit Scores to Job Applications: California's Reparations Task Force Looks to Algorithms*, KQED (Feb. 3, 2022), https://www.kqed.org/news/11903718/from-credit-scores-to-job-applications-californias-reparations-task-force-looks-to-algorithms [https://perma.cc/H9JW-UTAM].

[290] *See What Is Data for Black Lives*, DATA FOR BLACK LIVES (Sept. 2, 2020), https://d4bl.org/videos/55-what-is-data-for-black-lives [https://perma.cc/B6RV-QLDE].

[291] *See* Paul Watkins, *Introducing #NoMoreDataWeapons*, DATA FOR BLACK LIVES (Feb. 26, 2021), https://d4bl.org/dispatch/72-introducing-no-more-data-weapons [https://perma.cc/8GJU-L4GA].

[292] Ruha Benjamin & Jasmine McNealy, *A New Jim Code?*, HARVARD UNIV.: BERKMAN KLEIN CTR. (Sept. 24, 2019), https://cyber.harvard.edu/events/new-jim-code [https://perma.cc/PB8M-VN5Z].

VI. CONCLUSION

Criminal records are a ubiquitous part of American society, ranging from employment and housing screening tools, for building online content, for local news and community watch, and for internal systems in policing, sentencing, and immigration. But this reliance on criminal records as a purportedly helpful information source is clouded by the significant evidence showing how inaccurate this information can be to people marked with a criminal record.

Inaccuracies are exacerbated by the private sector, which is led by a set of incentives that promote even less accuracy—cost effectiveness is prioritized over accuracy, and companies can rely on most background check subjects never contesting their results due to the significant legal obstacles that stand in their way. Plus, a mixed yet widely permissive policy landscape means siloed and often mismatching criminal record information is widely available to the general public.

This Article aimed to problematize and describe criminal record accuracy in a concrete way, detail the legal obstacles that both prevent better criminal record data practices and prevent harmed people from remedy, and offer technical and broad scale responses that might, in turn, elevate the harms of data accuracy as a key issue for criminal legal system reform.