9-15-2020

POVERTY LAWGORITHMS A Poverty Lawyer's Guide to Fighting Automated Decision-Making Harms on Low-Income Communities

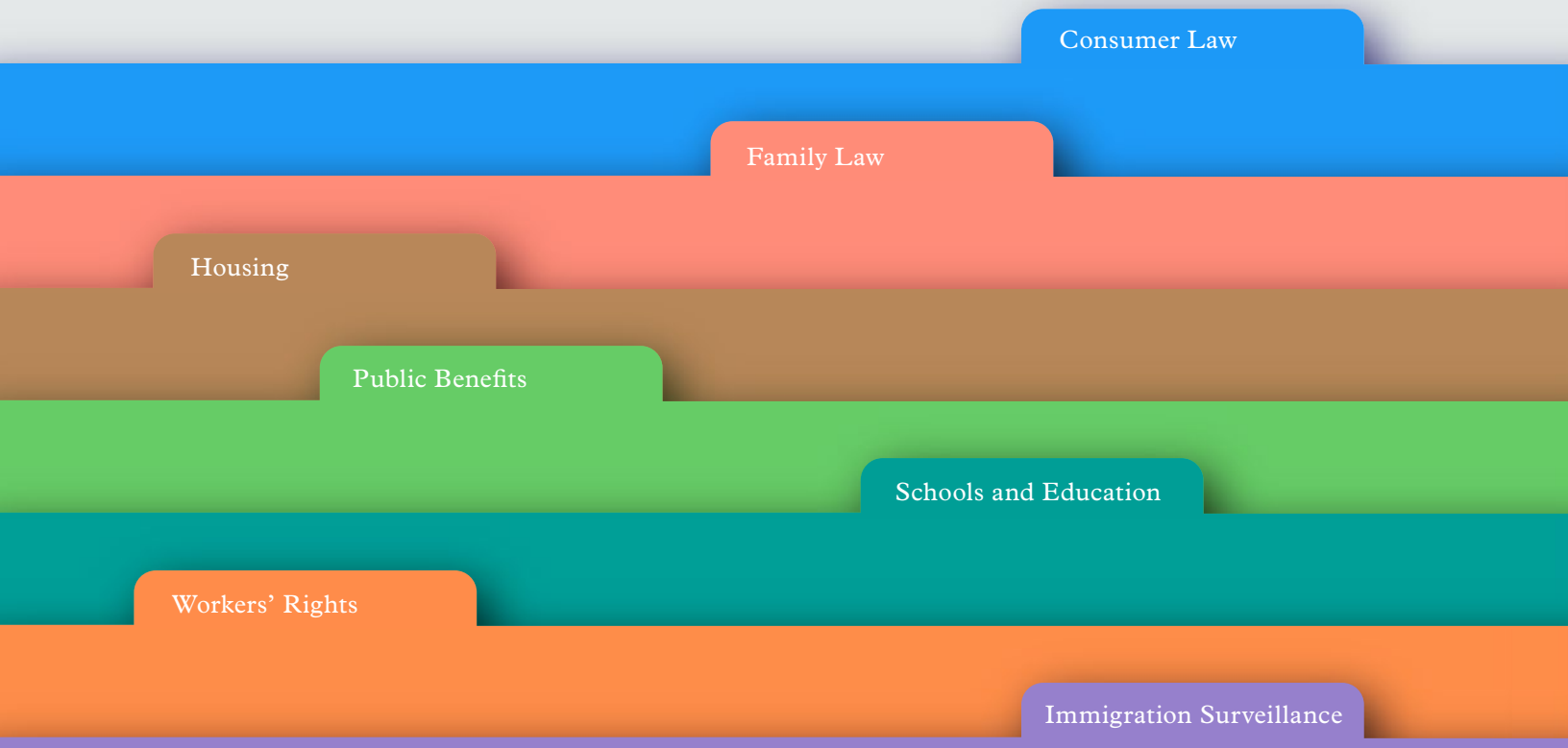
Michele E. Gilman
University of Baltimore School of Law, mgilman@ubalt.edu

DATA&
SOCIETY

POVERTY LAWGORITHMS

A Poverty Lawyer's Guide to Fighting Automated Decision-Making Harms on Low-Income Communities

Michele Gilman



PREFACE

We live in a "datafied" society in which our personal data is constantly harvested, analyzed, and sold by governments and businesses. Algorithms analyze this data, sort people into categories, and serve as gatekeepers to life's necessities. Yet people remain largely in the dark about these big data systems, creating an informational asymmetry whose harmful consequences fall most harshly on low-income people. Data-centric technologies add scope, scale, and speed to negative inferences about poor people. Based on their digital profiles, they can find themselves excluded from mainstream opportunities, such as jobs, education, and housing; targeted for predatory services and products; and surveilled by systems in their neighborhoods, workplaces, and schools. The technological systems impacting low-income communities raise profound issues of civil rights, human rights, and economic justice.

As a result, civil legal services (or poverty) lawyers increasingly represent clients whose legal challenges are intertwined with automated decision-making systems, digital profiling, predictive analytics, and various artificial intelligence tools. Competent legal representation requires an ability to issue-spot the ways in which data-centric technologies intersect with legal claims and defenses and to understand governing legal frameworks. At the same time, lawyers do not need the technical expertise of computer scientists to effectively interrogate these systems. Rather, understanding where and how data-centric technologies operate puts lawyers in a powerful position to advocate alongside their clients.

This report is designed to help poverty lawyers and their clients resist the adverse impacts of data-centric technologies and to engage as stakeholders in the adoption and implementation of algorithmic systems. The report is organized by major practice area and includes links to helpful resources for deeper dives into specific issues that may arise in legal services representation and policy advocacy. The practice areas covered are **consumer**, **family law**, **housing**, **public benefits**, **schools and education**, and **workers' rights**, as well as a final section on how **immigration surveillance** intersects with these practice areas. The report aims to assist legal services attorneys in identifying the impacts that existing and emerging technologies have on their clients. It does not cover the myriad ways attorneys and scholars have challenged algorithmic systems in the criminal justice system, although it is deeply indebted to their insights.

"Data-centric technologies add scope, scale, and speed to negative inferences about poor people."

CONTENTS

FOUNDATIONAL CONCEPTS

DEFINITIONS

Before delving into substantive practice areas, some core definitions are essential to understanding the data-centric technologies that impact legal services clients.

An **algorithm** is a set of well-defined instructions, especially for use by a computer. In the context of automated decision-making, an algorithm is the set of instructions that tells a computer how to complete a prespecified task. **Automated decision-making** is a way to divide complex decisions into discrete tasks that a computer algorithm or set of algorithms can perform on digital data.

Algorithms can range from the very simple to the very complex. Some algorithms are **rule based**, meaning the problem space and potential solutions are discrete and predefined. The computer does exactly what the programmer asks it to do. A food stamp calculator is an example of this type of algorithm.

Other algorithms are used in **machine learning**, which may or may not be rule based. "Machine learning" refers to a broad range of algorithmic techniques, including simple statistical analyses as well as cutting-edge techniques known as "deep learning" or "neural networks." In the most basic sense, machine learning is an automated process in which a computer analyzes large sets of data to discover correlations in existing data, which can then be used to make predictions about future behavior. All but the most advanced forms of machine learning rely on prespecified models to analyze the data. While designers of machine learning systems can't necessarily specify or even predict every outcome, the system's overall performance is very much shaped by designers—from the datasets and models used to the selection of tasks and goals the algorithms are addressing. When Netflix recommends certain movies to viewers, it is making these predictions based on a form of machine learning. Certain fraud detection systems in public benefits regimes also rely on machine learning to identify suspicious patterns within data sets. Machine learning is one type of **artificial intelligence (AI)**. AI is a broad category of technologies that attempts to approximate human intelligence.

Digital profiling is the automated processing of personal data in order to evaluate people and/or to predict their behavior. Algorithms are used in profiling. A credit score is an example of profiling, as is a tenant screening report.

GUIDING PRINCIPLES

Six overarching principles pertain to all civil practice areas. The first is that **digital technologies are impacting legal services clients**. Unfortunately, many lawyers and their clients are unaware of these automated decision-making systems. An informal, national survey of legal services lawyers and staff found that 0% of respondents believed that automated systems or AI was "very frequently" used in benefits applications, while 45% were unsure whether their clients were subject to automated decision-making. The actual rate of automated eligibility determinations in benefits systems is much higher, if not 100%. This is because automated systems are used in all states

to determine public benefits eligibility and to maintain data on applicants, and the vast majority of low-income people interact with government assistance programs.

Many automated decision-making systems operate invisibly and without opportunities for public input. An applicant for rental housing, for instance, may be denied based on an algorithmic determination in a tenant screening report yet never learn about the basis of the denial. In addition, governments regularly adopt automated decision-making systems without public knowledge or input. For many years, a sharp digital divide between poor people and more affluent Americans meant that wealth determined access to computers and the internet. However, that divide is narrowing, largely due to increased smartphone access. At the same time, businesses and government have become vastly ore sophisticated in monetizing and utilizing personal data. Thus, lawyers who learn to look for these issues will begin to see them throughout their dockets.

Second, lawyers need to understand that **computers are not magic**.[1] It is tempting to put faith in computers given the biases and errors associated with human decision-making. In contrast to humans, computers appear objective and accurate. However, people program computers and import human biases and errors into computer models, thus, the computer science saying, "garbage in, garbage out." As author and math professor Hannah Fry states, "Algorithms are a lot like magical illusions. At first they appear to be nothing short of wizardry, but as soon as you know how the trick is done, the mystery evaporates."[2] Poverty lawyers must understand how systems use algorithms in ways that can harm clients.

In creating an algorithm, developers exercise human judgment at numerous points. People determine and define the algorithm's goals and desired outputs; they identify, collect, and clean the data that feeds the models; they select and apply an algorithmic model; they screen results for errors and outliers and tweak the model accordingly; they set the acceptable levels of false negatives and false positives; and they interpret a model's outcomes. Mistakes and biases can be incorporated at any and all of these stages.

For instance, the data that algorithms analyze can contain errors. Any lawyer who has reviewed a credit report with a client has seen the range of errors and omissions that can be baked into a credit score, which is a type of algorithmic output. In the unregulated data broker industry, errors are even higher, typically no more accurate than a coin toss. Data, or information, brokers are companies that scrape personal data from multiple sources, aggregate the data to create personalized digital profiles, and sell the profiles to a variety of industries and government agencies.

Mistakes also arise when programmers inaccurately translate regulatory requirements into source code—an outcome that won't surprise lawyers who regularly wrestle with complex and ambiguous regulations in fields such as public benefits, the environment, or tax. Millions of Americans have lost access to desperately needed public benefits as a result of coding errors.[3] In addition, some concepts regularly embedded into law, such as reasonable, necessary, and credible, require human judgment and are thus difficult, if not impossible, to translate into code.

1 M.C. Elish & danah boyd (2018), *Situating Methods in the Magic of Big Data and AI*, Communication Monographs 85:1, 57, https://www.tandfonline.com/doi/abs/10.1080/03637751.2017.1375130?needAccess=true&journalCode=rcmm20.

2 Hannah Fry, *Don't Believe the Algorithm*, Wall St. J., Sept. 5, 2018, https://www.wsj.com/articles/dont-believe-the-algorithm-1536157620.

3 Danielle Keats Citron, *Technological Due Process*, 85 Wash. U. L. Rev. 1249 (2008).

Another reason for caution is that data is not neutral. Data sets reflect structural inequities, which in turn can result in digital discrimination against marginalized groups.[4] Just as rotten eggs will spoil a recipe, bad or incomplete data spoils algorithmic outcomes. For instance, a commercial health care algorithm was identifying white patients for more intensive medical care than similarly ill Black patients.[5] The algorithm was shown to rely on data about past health care expenditures to make predictions about patients' future needs. As health care lawyers are well aware, African Americans suffer numerous logistical, institutional, and cultural barriers to health care access and thus have lower cost histories. When researchers reformulated the algorithm to eliminate past expenditures as a proxy for needs, the racial bias disappeared. These sorts of structural biases along class, race, and gender lines are endemic in the data that gets fed into algorithmic systems, thereby yielding unequal outcomes.

Third, despite the fallibility of algorithms, lawyers may confront judges, juries, and other **decision-makers inflicted with automation bias**. This is a psychological phenomenon in which people defer to computer-generated outputs as more reliable than their own judgment.[6] In one study, the vast majority of participants who believed they were in a room on fire followed instructions from a robot pointing to an obscured route rather than taking clearly marked exits.[7] In the justice system, the concern is that judges and juries will yield to algorithmic determinations without adequate context or skepticism. Alternatively, lawyers and judges may be skeptical of algorithms but still use these data-centric tools to mask their subjective decision-making, "burying them under a patina of objectivity and making them harder to monitor."[8] In either situation, poverty lawyers need the tools to understand why algorithms can be incorrect, to access and interrogate algorithmic models, and to explain to judges and other decision-makers why they should neither blindly trust nor completely reject an algorithmic determination.

Fourth, in challenging algorithms in adversarial proceedings, poverty lawyers are likely to **face claims that the algorithm is proprietary**. Under state laws, businesses gain trade secret protection for nonpublic information that gives them a competitive advantage if they take reasonable efforts to maintain secrecy. Further, many government agencies that purchase algorithmic software from private vendors do so under contractual, nondisclosure agreements. Nevertheless, in the civil context,[9] courts have ruled that procedural due process interests prevail over trade secrecy claims in cases involving algorithms that determined Medicaid

4 Center for Democracy and Technology, *AI and Machine Learning*. For an overview of the ways big data can harm marginalized communities, see Mary Madden, Michele Gilman, Karen Levy, & Alice Marwick, *Privacy, Poverty and Big Data: A Matrix of Vulnerabilities for Poor Americans*, 95 Wash U. L. Rev. 53 (2017).

5 Ziad Obermeyer et al., *Dissecting Racial Bias in an Algorithm Used to Manage the Health of Populations*, Science, Oct. 25, 2019, https://science.sciencemag.org/content/366/6464/447.

6 L.J. Skitka, K.L. Mosier, & M. Burdick, *Does Automation Bias Decision-Making?*, 51 Int'l J. of Human-Computer Studies, 991 (1999)..

7 Aviva Rutkin, *People Will Follow a Robot in an Emergency – Even if It's Wrong*, New Scientist, Feb. 29, 2016, https://www.newscientist.com/article/2078945-people-will-follow-a-robot-in-an-emergency-even-if-its-wrong.

8 Angéle Christin, *Algorithms in Practice: Comparing Web Journalism and Criminal Justice*, Big Data & Society 1 (July–Dec. 2017), https://journals.sagepub.com/doi/pdf/10.1177/2053951717718855.

9 Results have been more mixed in criminal cases. *See* Rebecca Wexler, *Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System*, 70 Stanford L. Rev. 1343 (2018).

care levels[10] and teacher performance ratings.[11] This is a new and evolving area of the law.

Other levers for algorithmic disclosure are also possible, particularly where government agencies are using algorithms in decision-making. Freedom of information laws can be used to request where and how government agencies use algorithms, as well as to seek information about how the models operate, although the scope of statutory exceptions remains in flux and is likely to be litigated in coming years.[12]

Another route for disclosure is to monitor state and local procurement processes as governments purchase algorithmic tools for carrying out government services.[13] In addition, poverty lawyers and their clients can advocate for legislation to improve transparency around the adoption of automated decision-making systems. For instance, Washington State is considering an algorithmic accountability law that would establish procurement guidelines for automated decision-making systems; New York City adopted an algorithmic accountability law that created a task force to issue recommendations for city purchase and use of algorithms; and Seattle requires public disclosure, community engagement, and ongoing reporting when surveillance systems are purchased. These transparency efforts and others emerging across the country provide templates for consideration in other jurisdictions.

Fifth, poverty lawyers **do not need a technical background** or the ability to code software in order to effectively advocate in cases involving data-centric technologies. These emerging issues are no more complex than other interdisciplinary areas that poverty lawyers regularly have to master to effectively represent clients, such as the health effects of lead paint and remediation requirements, permissible credit financing structures under federal and state lending laws, and the feasible educational and therapeutic strategies for students receiving special education services. With regard to data-centric technologies, there are many available resources (including those linked in this report) and experienced lawyers who have challenged algorithmic systems and can provide guidance. Moreover, by gaining the skills to issue spot digital privacy issues, lawyers will be well situated to connect with technical experts where necessary.

Finally, while outside the scope of this report, **technology is bringing many benefits** to low-income people, legal services practices, and the justice system. Internet access gives low-income people the ability to apply for jobs or services and to connect with social justice movements with ease. Antipoverty advocates have developed tech tools to empower low-income communities, such as smartphone apps that keep track of hours worked for purposes of wage claims, automatically complete expungement petitions, and provide *pro se* legal advice. They have also analyzed open data, such as eviction data, to understand outcomes and advocate for systemic

10 K.W. v. Armstrong, 180 F. Supp. 3d 703 (D. Idaho 2016).

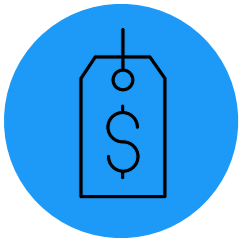
11 Hous. Fed'n of Teachers, Local 2415 v. Hous. Indep. Sch. Dist., 251 F. Supp. 3d 1168, 1175–80 (S.D. Tex. 2017). The Court explained that the developer's "trade secrets do not empower, much less compel, [the school district] to violate the constitutional rights of its employees." *Id*. at 1179.

12 *See* Robert Brauneis & Ellen P. Goodman, *Algorithmic Transparency for the Smart City*, 20 Yale J. L. & Tech. 103 (2018); Hannah Bloch-Webha, *Access to Algorithms*, 88 Fordham L. Rev. 1265 (2020); *Algorithmic Accountability Policy Toolkit,* AI Now Institute (Oct. 2018), (including a model public information act request).

13 *Id*. at 11 (including model procurement language).

change. The legal services community is considering how to use technology to improve legal representation and the justice system. Continued innovations may well assist in combating the harms identified in this report.

CONSUMER LAW



Consumer lawyers regularly assist clients with the consequences of credit and consumer reports, which are based on digital scraping of personal data. These reports determine access to housing, jobs, and education. Technology is also reshaping the debt collection industry and making it easier to target and exploit vulnerable consumers.

CONSUMER REPORTING

Consumer reporting agencies, data brokers, internet platforms, digital advertising companies, and other businesses are making millions of dollars compiling and selling consumers' digital profiles.[14] Personal data is gathered from a multitude of sources, including public records, web browsing activity, emails, banking activity, social media, store loyalty cards, online quizzes, license-plate readers, app usage, smart devices (such as fitness watches and internet-connected doorbells), and geolocation tracking on smartphones. Personal profiles are also shaped by data pulled from their online networks; in other words, they are judged by their social media friends. From all this data, businesses glean people's buying habits, social relationships, creditworthiness, political preferences, lifestyle, hobbies, health, and personality—and even make predictions about their future behavior. These networks of data extraction lack transparency and accountability and raise the risks of digital discrimination and inaccuracy.

Consumer reports are nothing new; they have been assembled for decades as a way of assessing a consumer's creditworthiness. However, the scope and scale of today's data markets are much vaster, much faster, and more granular. The dangers for low-income people arise because digital profiles often operate as gatekeepers to affordable credit, jobs, employment, education, insurance, health care, and other life

14 Federal Trade Comm'n, Data Brokers: A Call for Transparency and Accountability (May 2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

necessities. They are also used to target low-income people with predatory marketing schemes, such as payday loans and for-profit educational scams.

For people living on the economic margins, credit reports can be economically devastating because, as consumer attorney Chi Chi Wu has stated, they penalize "consumers who have fallen on hard times through no fault of their own—from illness, job loss, victims of fraud, or victims of natural disasters, treating them as irresponsible deadbeats."[15] These consumers can find themselves in a vicious cycle in which their failure to pay a bill becomes encoded in their digital profile, which in turn makes it difficult to get a job or pay rent, which in turn worsens their hope of paying their bills and improving their credit standing.[16] These cycles fall most harshly on communities of color, due to structural disadvantages in the economy.[17]

At the other extreme of the data extraction spectrum, 44 million people are "credit invisible" because they are disconnected from mainstream financial services and thus do not have a credit history. For these consumers, credit reporting agencies and the financial technology industry are exploring using alternative data points for scoring, such as rental payment history, utility payments, or bank account information. Some of these alternatives are likely helpful to low-income consumers, while others will prove harmful.[18] The devil is in the details and thus will require careful attention from and involvement of consumer attorneys.[19]

"The dangers for low-income people arise because digital profiles often operate as gatekeepers to affordable credit, jobs, employment, education, insurance, health care, and other life necessities."

The primary statute governing consumer reporting is the Fair Credit Reporting Act (FCRA).[20] Under FCRA, consumer reporting agencies (CRA) must adopt reasonable procedures to ensure the accuracy of the information they report. CRAs include the big three credit bureaus: Experian, Equifax, and TransUnion. These are private companies beholden to shareholders and whose customers are primarily creditors and debt collectors; thus, the interests of low-income consumers

15 Testimony of Chi Chi Wu, National Consumer Law Center, before the U.S. House of Representatives Comm. on Financial Svcs., *"Who's Keeping Score? Holding Credit Bureaus Accountable and Repairing a Broken System"* (Feb. 26, 2019), https://www.nclc.org/images/pdf/credit_reports/testimony-hfsc-credit-reporting-hearing.pdf.

16 Chi Chi Wu, *Solving the Credit Conundrum: Helping Consumers' Credit Records Impaired by the Foreclosure Crisis and Great Recession*, National Consumer Law Center (Dec. 2013), https://www.nclc.org/images/pdf/credit_reports/report-credit-conundrum-2013.pdf.

17 National Consumer Law Center, Past Imperfect: How Credit Scores and Other Analytics "Bake In" Past Discrimination and Perpetuate It (May 2016), https://www.nclc.org/images/pdf/credit_discrimination/Past_Imperfect050616.pdf.

18 Testimony of Wu, *supra* note 15, at 9–10.

19 *Id.*; *see also* Matthew Adam Bruckner, *The Promise and Perils of Algorithmic Lenders' Use of Big Data*, 93 Chi.-Kent L. Rev. 3, 18–29 (2018).

20 15 U.S.C. §§ 1681–1681x.

are not part of their business model.[21] (For this reason, some advocates have called for establishing a public credit registry.[22])

According to the FCRA, CRAs also include any entities that prepare reports that bear "on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living" and are used for purposes of credit, insurance, or employment, and certain other eligibility determinations. Employment and tenant screening companies, then, are CRAs, while digital profiles used for marketing are not. Reports prepared by data brokers may fall within FCRA's coverage depending on the purposes for which they are sold. Still, several data brokers have successfully convinced courts that their activities fall outside FCRA's scope, even though they engaged in activities in covered areas.[23] Consumer lawyers should consider that data brokers eliding FCRA coverage may open themselves up to litigation under state law claims, such as defamation, invasion of privacy, or negligence, which are otherwise preempted under FCRA.[24]

Consumer rights under FCRA are straightforward, if inadequate. Consumers must be given an adverse action letter when, based on a consumer report, they are denied or offered worse terms for credit, insurance, employment, or housing. The letter must contain the contact information of the entity that supplied the information and notice of rights to dispute the accuracy and completeness of the information in the report. Consumers can also obtain free copies of their credit reports (one per CRA per year), and identity theft victims and unemployed persons have additional rights to free credit reports.

Consumers have rights to correct inaccurate and outdated information in consumer reports, although these processes can be cumbersome and frustrating due to automated systems that usually rubber-stamp the findings of the furnishers, which are the companies that provide data to the credit bureaus, such as creditors and debt collectors.[25] The Federal Trade Commission (FTC) provides self-help guidance to consumers for correcting information in a credit report in its document, *Credit Repair: How to Help Yourself*. If these remedies are not sufficient, consumers can file litigation against CRAs that negligently or willfully fail to comply with their FCRA obligations. This area of the law can be highly technical, but the National Consumer Law Center (NCLC) publishes comprehensive treatises that detail available litigation remedies.

Private rights of action are essential because consumer report inaccuracy is a major problem. The FTC has reported that one in five Americans has an error on their credit report and that one in twenty have errors

21 National Consumer Law Center, Fair Credit Reporting 1.2.2 (9th ed. 2017), updated at https://www.nclc.org/library.

22 Amy Traub, *Establish a Public Credit Registry*, Demos (2019), https://www.demos.org/sites/default/files/2019-03/Credit%20Report_Full.pdf.

23 *Id*. at 2.5.3.2.

24 Chi Chi Wu, *Data Gatherers Evading the FCRA May Find Themselves Still in Hot Water*, National Consumer Law Center, June 14, 2019, https://library.nclc.org/data-gatherers-evading-fcra-may-find-themselves-still-hot-water.

25 Chi Chi Wu, Michael Best & Sarah Bolling Mancini, *Automated Injustice Redux: Ten Years After a Key Report, Consumers Are Still Frustrated Trying to Fix Credit Reporting Errors*, National Consumer Law Center (Feb. 2019), https://www.nclc.org/images/pdf/credit_reports/automated-injustice-redux.pdf.

"Unfortunately, even if an individual obtains an order of expungement, the underlying criminal record may already have been scraped by a data broker and included in various consumer reports and other digital profiles."

serious enough to result in the denial of credit or higher credit costs.[26] The accuracy of reports compiled by data brokers is even lower. In light of the shortcomings in the credit reporting industry, the NCLC has called for reforms,[27] including consumer rights to appeal, stricter data-matching criteria, more thorough investigations, injunctive relief for consumers, and a public credit reporting system. Even if credit reporting accuracy improves, FCRA's protections are not substantive. "So long as a data broker or employer complies scrupulously with the disclosure requirements, the FCRA imposes very few substantive limits on the types of information that can be collected or disclosed."[28] As a result, "FCRA does little to restrict the vast data gathering that occurs or to protect against the sharing of highly personal or sensitive information."[29]

States are beginning to legislate for more substantive consumer data protection. In Vermont, data brokers must register with the state annually, maintain data security standards, and refrain from fraudulently acquiring certain types of data or using data for harassment or discrimination.[30] In California, the California Consumer Privacy Act (CCPA)[31] —the first comprehensive privacy legislation in the United States—gives consumers rights to know what data companies are collecting about them, to opt out of having their information sold to third parties, and to request that a company delete their personal information. CRAs are exempt from the CCPA due to their coverage under FCRA, but data brokers falling outside FCRA are covered. Numerous states and Congress are considering bills to enhance consumer control over their personal data, resulting in many opportunities for low-income consumer advocacy in coming years.

CRIMINAL RECORDS AND EXPUNGEMENT

A troublesome aspect of consumer reporting involves the inclusion of criminal records, including records that have been expunged or sealed. Every state has an expungement and/or sealing statute that permits certain criminal records to be deleted from the official state record. Expungement statutes are designed to reduce the collateral consequences of having a criminal record. One in three Americans has a criminal record, and

26 Federal Trade Comm'n, Report to Congress Under Section 319 of the Fair and Accurate Credit Transactions Act of 2003 (Dec. 2012), https://www.ftc.gov/sites/default/files/documents/reports/section-319-fair-and-accurate-credit-transactions-act-2003-fifth-interim-federal-trade-commission/130211factareport.pdf.

27 Testimony of Wu, *supra* note 15.

28 Pauline T. Kim & Erika Hanson, *People Analytics and the Regulation of Information Under the Fair Credit Reporting Act*, 61 St. Louis U. L.J. 17, 32 (2016).

29 *Id.*

30 9 Vt. Stat. Ann. § 2430 *et seq.*

31 Cal. Civ. Code § 1798.100 *et seq.*, eff. Jan. 1, 2020.

despite the lack of a conviction (as is true of the majority of criminal records), the collateral consequences can result in decreased access to jobs, housing, education, and other resources. Unfortunately, even if an individual obtains an order of expungement, the underlying criminal record may already have been scraped by a data broker and included in various consumer reports and other digital profiles. Many consumer reporting and background check companies lack procedures to update or verify expunged criminal records. These failings violate FCRA's accuracy requirements, but they can be hard to uncover and time-consuming to remedy.

Tracing and removing all mentions of an expunged record are difficult. Says attorney Sharon Dietrich, "As I advise clients, hopefully they will no longer be affected by the expunged case, but they should think of expungement like ants in their kitchen; you may think you've got them all only to later discover that one or two have escaped under the refrigerator."[32] There are a variety of steps to try to capture the ants, including sending expungement orders to large credit reporting companies, requesting criminal background check files from the list of companies maintained by the Consumer Financial Protection Bureau, filing complaints with the bureau or the FTC, and pursuing FCRA litigation.[33]

States can also do more to fulfill the purpose of their expungement statutes. For instance, in Pennsylvania, (as a matter of contract) the Administrative Office of the Courts requires that bulk purchasers of court records follow a lifecycle file approach, maintaining accurate updates regarding criminal records and submitting to court audits. Minnesota has a similar approach.[34] This proactive and enforceable solution, placing the burden on the purchaser, is ideal and should be pursued nationwide.

Criminal records that are not expungable are also deeply problematic. Even if they are accurate, they can be a barrier to economic opportunity and public assistance, particularly for people of color, who bear a disproportionate burden of mass criminalization policies.[35] Criminal background screening (a form of consumer reporting) is used by 87% of employers, 80% of landlords, and 66% of colleges.[36] This has led to ban-the-box policies for job and college applicants; these policies generally restrict questioning about criminal history on initial applications, while permitting criminal background checks later in the process when there are opportunities for more individualized assessments. The Department of Housing and Urban Development (HUD) encourages individualized assessments in the housing context, and the Equal Employment Opportunity Commission has issued guidance for employers on how to handle criminal records. The use of criminal records in employment and education is addressed in more detail in subsequent sections of this report.

32 Sharon M. Dietrich, *Ants Under the Refrigerator? Removing Expunged Cases from Commercial Background Checks*, Criminal Justice 26 (Winter 2016), https://clsphila.org/wp-content/uploads/2019/10/Ants-under-the-Refrigerator-published.pdf.

33 *Id.*

34 Consumer Financial Protection Bureau, Market Snapshot: Background Screening Reports: Criminal Background Checks in Employment 16 (Oct. 2019), https://files.consumerfinance.gov/f/documents/201909_cfpb_market-snapshot-background-screening_report.pdf.

35 Angela Hanks, *Ban the Box and Beyond*, Center for American Progress (July 27, 2017), https://www.americanprogress.org/issues/economy/reports/2017/07/27/436756/ban-box-beyond.

36 Dietrich, *supra* note 32, at 26.

AUTOMATED DEBT COLLECTION

Debt collection is increasingly automated.[37] To urge debtors to pay, debt collectors deploy automated calls (a.k.a., robocalls), texts, emails, and outreach on social media. They offer online platforms that feature live help or avatars to engage in consumer communications, negotiations, and payment collection. They use software that can not only predict the best mode of communication for a given debtor but also analyze speech patterns and deliver personalized content or tone. Debt collectors have technology that delivers prerecorded messages to voice- mail without causing the phone to ring, identifies when people (as opposed to voice mail) answer phones, and use caller ID spoofing to mask the nature of calls.

Debt collectors also use software to manage accounts, oversee the collection process, and track consumer discussions and collection activity. To boost their productivity, they have adopted video game style techniques that let agents view their own performance and compete with other agents. Collection analytics help debt collectors decide which debt portfolios to buy, monitor changes in consumer payment ability, target consumers most likely to pay, and scrub certain accounts, such as those indicating bankruptcy, death, or litigious debtors. The NCLC warns that "the use of analytics raises questions about privacy, disparate treatment based on demographic data like race or gender, and the potential for unauthorized use of credit report data."[38]

Consumers can be barraged by these automated systems. Indeed, "more than half of the top 20 spam callers... are categorized as debt collection callers."[39] Debt collection activities comprise the majority of complaints to the FTC. The debt collection industry affects millions of people: about one-third to one-quarter of adults with a credit report has a debt in collection, with medical debt accounting for more than half of these debts.[40]

There are legal remedies to fight debt collection harassment. The national Fair Debt Collection Practice Act prohibits repeated and continuous calls "with intent to annoy, abuse, or harass any person at the called number."[41] Debt collectors cannot call consumers at work, call outside the hours of 8 a.m. to 9 p.m., reveal debt to third parties, mispresent stale debts as timely, obtain information about consumers through false pretenses, or make false claims about their identity or the consequences of failing to pay a debt. Collectors also must cease contact with a consumer when they are represented by an attorney or when they have written a cease contact letter. A consumer also has the right to demand verification of the debt. Fines for violations can be significant.

37 *See* National Consumer Law Center, Fair Debt Collection 1.5.5 (9th ed. 2018),; Consumer Financial Protection Bureau, Study of Third Party Debt Collection Operations 24–25, 32–34 (July 2016), https://files.consumerfinance.gov/f/documents/20160727_cfpb_Third_Party_Debt_Collection_Operations_Study.pdf.

38 National Consumer Law Center, Fair Debt Collection 1.5.5 (9th ed. 2018), updated at http://www.nclc.org/library.

39 Federal Communications Comm'n, Report on Robocalls (Feb. 2019), https://docs.fcc.gov/public/attachments/DOC-356196A1.pdf.

40 Comments on CFBP proposed debt collection rules from consumer, civil and human rights, labor, community and legal services organizations, Docket No. CFPB-2019-0022 (Sept. 18, 2019), https://www.nclc.org/images/pdf/debt_collection/coalition-comments-debt-collection-sept2019.pdf.

41 15 USC § 1692d.

"Digital profiling makes it easier for predatory businesses to identity and target low-income consumers with unfair and abusive loan terms."

In addition, the Telephone Consumer Protection Act (TCPA) forbids the use of auto-dialed and prerecorded calls to cell phones. This is helpful because low-income consumers are more likely to rely on cell phones than landlines. Impermissible calls include those related to debt collection and subject violators to liability of $500 per call or $1,500 for willful violations. There are some grey areas involving whether the act covers new technologies that have been designed expressly to evade the TCPA's coverage. There are also legal uncertainties around whether consumers in certain situations have consented to the calls (which is an exception to the ban), although there is consensus that consumers can easily revoke any prior consent.

In short, consumers facing harassing or invalid debt collection contacts have a variety of legal remedies, although concerns around possible discrimination, lack of data security, and the sale or other uses of credit data require ongoing systemic attention and advocacy.

PREDATORY LENDING

Digital profiling makes it easier for predatory businesses to identity and target low-income consumers with unfair and abusive loan terms. Payday lending is one prime example, with a significant online presence. A payday loan is a short-term, unsecured, high-interest loan that is repayable with the borrower's next paycheck. The average annual percentage rate (APR) for online payday loans is 650%.[42] Due to high interest rates, borrowers struggle to pay back the loans, and 80% of payday loans are taken out to cover prior loans,[43] resulting in a debt trap. Every year, 12 million Americans take out payday loans, incurring $9 billion in loan fees.[44] The average income of borrowers is $30,000, and 58% of those borrowers struggle to meet monthly expenses.[45]

Eighteen states have effectively outlawed payday lending; many others regulate the industry; and all ban deceptive practices in connection with payday lending. This tighter regulatory environment, along with the potential of enhanced profits, has pushed the industry to market aggressively online.[46] Seventy-five percent of online loans are initiated by lead-generation websites, which advertise the payday loans, collect consumer information through online forms, and then sell the sales leads (potential customers) to lenders.[47] Many consumers land on lead-generator websites after

42 The Pew Charitable Trusts, Fraud and Abuse Online: Harmful Practices in Internet Payday Lending (Oct. 2014), https://www.pewtrusts.org/-/media/assets/2014/10/payday-lending-report/fraud_and_abuse_online_harmful_practices_in_internet_payday_lending.pdf.

43 The Pew Charitable Trusts, *Payday Loan Facts and the CFBP's Impact* (Jan. 14, 2016), https://www.pewtrusts.org/en/research-and-analysis/fact-sheets/2016/01/payday-loan-facts-and-the-cfpbs-impact.

44 *Id.*

45 *Id.*

46 National Consumer Law Center, Consumer Credit Regulation § 9.6.2 (2d ed. 2015), updated at .

47 Pew, Fraud and Abuse, *supra* note 42, at 5; Upturn, Led Astray: Online Lead Generation and Payday Loans (Oct. 2015), https://www.upturn.org/reports/2015/led-astray.

being targeted with ads based on their digital profiles.[48] Although Google and Facebook have officially banned ads for payday loans from their platforms, the lending industry has found loopholes for reaching consumers online.[49]

Internet payday lenders typically seek borrower's authorization for electronic debits, electronic access to the borrower's bank account, or payment from remotely-created checks. Many internet-based loans are structured to ensure that they automatically roll over and incur additional fees, thus ensuring long-term indebtedness.[50] Overall, online payday loans tend to have worse terms than storefront loans: "They are associated with higher fees, longer-term indebtedness, higher rates of borrower abuse, and startling rates of fraud."[51] In addition, 30% of borrowers of online payday loans report being threatened by a lender or debt collector, at higher rates than storefront borrowers do.[52]

There are numerous scams involving websites that use consumer information to purchase unwanted services, trick consumers into paying nonexistent debts, and sell consumers bogus debt relief services.[53] These scammers can be hard to hold accountable because they can be difficult, if not impossible, to locate. Consumers have legal protections from payday lending abuses at the federal and state levels. At the federal level, a variety of laws apply to payday lending. For instance, The Truth in Lending Act requires various lender disclosures; the Equal Credit Opportunity Act forbids discrimination in lending and requires specific notices to consumers; the Electronic Fund Transfer Act prohibits conditioning credit on the preauthorization of electronic fund transfers; and the Military Lending Act effectively bars payday lending to military service members and their families (by prohibiting loans of more than 36% APR). However, a previous rule requiring that lenders confirm borrowers' ability to pay was rescinded in 2020, and there are agency proposals pending to allow payday lenders to partner with banks to funnel loans and thereby evade state usury caps, a proposal that consumer advocates call rent-a-bank. Future regulation of this industry will hinge on the commitments of the governing administration.

At the state level, laws vary widely. Some states ban payday lending altogether, while others place limits on the amount of APR, the length of the repayment period, the percentage of a paycheck that can be withdrawn for repayment, or the maximum amount of the loan.[54] In most states, payday loans can be attacked as unconscionable or in violation of state unfair and deceptive acts and practices statutes. Notably, internet-based payday lenders must still comply with the law where their borrowers live. Many internet lenders are unlicensed in the states where they make loans, making their loans potentially unenforceable or partially void. Several state attorneys general have

48 *Id*. at 46.

49 *See* David Dayen, *Google Said It Would Ban All Payday Loan Ads. It Didn't,* The Intercept (Oct. 7, 2016), https://theintercept.com/2016/10/07/google-said-it-would-ban-all-payday-loan-ads-it-didnt.

50 Pew, Fraud and Abuse, supra note 42. "It violates the [Electronic Funds Transfer Act's] ban on mandatory electronic repayment to require recurring automatic electronic payments, whether rollovers of balloon payment loans or installment payments on longer-term loan." National Consumer Law Center, Consumer Credit Regulation, *supra* note 43, at 9.6.2.1.

51 Upturn, Led Astray, *supra* note 47, at Sec. 2.

52 Pew, Fraud and Abuse, *supra* note 42, at 1.

53 *Id*. at 27.

54 A list of state statutes regarding payday lending is available in Appendix B of the National Consumer Law Center treatise on Consumer Credit Regulation.

sued online lenders that have violated the rights of their citizens. Unfortunately, the lending industry is constantly developing new predatory products and practices to evade legal and advertising restrictions. For all these reasons, legal services clients struggling with payday loans should be counseled about other lending options.[55]

IDENTITY THEFT

In 2017, identity thieves stole $16.8 billion from 16.7 million consumers.[56] Credit card fraud is the most common form of identity theft; other forms include employment and tax-related fraud, and phone and utilities fraud.[57] Large-scale data breaches happen regularly, with CRAs among the targets. In 2017, hackers breached Equifax and gained access to the personal information (including names, social security numbers, driver's license numbers, birth dates, and addresses) of 168 million Americans. Equifax did not detect the breach for 76 days. Breaches are common—anyone who has ever shopped at Target, Marshalls, or Home Depot; ridden in an Uber; stayed at a Marriott; banked at JPMorgan Chase or Capital One; connected on Facebook; played games on PlayStation; shopped on eBay; had a Yahoo account; been employed by the federal government; or had a credit card has had a potential data breach.

Identity theft is a scary proposition, regardless of income level, because of the potential economic losses and associated stress. As the NCLC warns, "Once the impostor has established himself or herself as the consumer, the impostor may leave unpaid credit cards, cleaned-out checking accounts, foreclosed mortgages, default judgments, bankruptcy declarations, stolen tax refunds, and (at worst) arrest warrants all firmly stuck to the consumer's financial identity."[58] Moreover, the average identity theft victim spends 60 hours and over $1,300 managing the consequences. However, the aftermath can play out more harshly for low-income people, who have fewer resources to manage the financial ripple effects of identity theft. Legal aid lawyers have seen clients struggle with utility shutoffs, mistaken arrests, and incorrect child support enforcement orders after their clients' identity is misappropriated by someone else.[59]

The 700,000 children in foster care are particularly vulnerable to identity theft due to the ready availability of their personal information as they move through the foster care system and come into contact with numerous social workers, group homes, foster families, and relatives.[60] This is compounded by the likelihood of non-detection of theft for many years.[61] With damaged credit, former foster youth can find themselves denied

55 Tobie Stanger, *CFPB Proposes to Relax Payday Loan Regulation*, Consumer Reports (Feb. 6, 2019), https://www.consumerreports.org/consumer-financial-protection-bureau/cfpb-bids-to-relax-payday-loan-regulation.

56 National Consumer Law Center, Fair Credit Reporting, *supra* note 21, at 9.1.1.

57 *Id.*

58 *Id.*

59 Sarah Dranoff, *Identity Theft: A Low-Income Issue*, American Bar Ass'n Dialogue (Dec. 15, 2014), https://www.americanbar.org/groups/legal_services/publications/dialogue/volume/17/winter-2014/identity-theft--a-lowincome-issue.

60 Lisa Weintraub Schifferle & Maria Del Monaco, *Stolen Future: Foster Youth Identity Theft*, 47 Clearinghouse Rev. J. of Pov. L & Pol'y 407 (Mar.–Apr. 2014). A study in Los Angeles found that eight percent of sixteen- and seventeen-year-olds were identity theft victims.

61 *Id.*

jobs, student loans, car loans, and cell phones.[62] A federal law requires the states to conduct annual credit checks for foster youth over the age of 14 and to fix any inaccuracies.[63] The law, however, is underenforced and can leave teens with unresolved credit issues when they age out of the system.[64]

In light of these impacts, it is thus not surprising that a national survey by Data & Society found that low-income people report higher levels of concern about loss or theft of their information, along with greater fears about being targeted for an internet scam or fraud.[65] In fact, they report higher rates of being victimized by online scams that result in financial losses.[66] Further, the lowest-income households are far less likely to use privacy-enhancing settings or strategies, such as avoiding sharing sensitive information online or turning off web browser cookies.[67] The digital privacy concerns of low-income people are intertwined with their offline fears regarding their physical safety.[68]

"...that low-income people report higher levels of concern about loss or theft of their information, along with greater fears about being targeted for an internet scam or fraud."

Victims of identity theft can request that CRAs block the reporting of fraudulent information in the consumer's file. This request triggers notification to the furnisher of the information, who must then conduct an investigation. Consumers can also report identity theft directly to creditors, which are prohibited from furnishing the information to CRAs. To prevent future identity theft, consumers can place security freezes or fraud alerts on their files at the big three CRAs, which will result in extra verification of identity when credit is sought in the consumer's name. A consumer can also take steps to notify retailers not to accept checks drawn on fraudulent accounts in the consumer's name. The specifics of these and related processes are described in detail in the NCLC treatise on Fair Credit Reporting and on the NCLC's website.

To the degree that CRAs and creditors fail to respond, FCRA provides private rights of action to enforce its specific protections for identity theft victims, as well as the more general FCRA rights for resolving disputed debts. There are also state remedies, such as filing criminal charges for identity theft, civil cases for fraud

62 Schifferle & Monaco, *supra* note 60, at 407–08.

63 2 U.S.C. 675(5)(I).

64 *See* Madison Howard Churchman, *A Clean Slate for Texas Foster Youth: Policy Recommendations on Preventing and Resolving Identity Theft for Youth in Foster Care*, 4 Tex. A&M J. Prop. L. 297, 311 (2018).

65 Mary Madden, *Privacy, Security, and Digital Inequality*, Data & Society (Sept. 27, 2017), https://datasociety.net/survey-research-low-ses-populations. In comparing the lowest-income households to the highest-earning households, concerns about loss or theft of financial information was 60% as compared to 38%; with regard to being victimized by an interest scam or fraud, the difference was 48% to 24%. *Id.* at 2. The highest rates of concerns regarding "financial, informational, and physical security" were from foreign-born Hispanic adults. *Id.* at 5.

66 *Id.* at 10. They report lower levels of theft of personal information. *Id.* Theft of health information is equal among income levels. *Id.*

67 *Id.* at 9.

68 *Id.* at 91.

and deception against identity thieves (although it's difficult to collect on a judgment from identity thieves), claims under the Uniform Commercial Code for bank negligence, and claims against government agencies that provided information to a thief.

CONSUMER RESOURCES

- Collateral Consequences Resource Center, http://ccresourcecenter.org/
- Federal Trade Commission, *Disputing Errors on Credit Reports*, https://www.consumer.ftc.gov/articles/0151-disputing-errors-credit-reports
- Federal Trade Commission, *Identity Theft: A Recovery Plan*, https://www.consumer.ftc.gov/articles/pdf-0009_identitytheft_a_recovery_plan.pdf
- National Consumer Law Center, Treatises on *Fair Debt Collection*, *Fair Credit Reporting*, and *Consumer Credit Regulation*, https://library.nclc.org/bookstore
- National Record Clearing Project, https://clsphila.org/national-record-clearing-project/
- Jenny Roberts, *Expunging America's Rap Sheet in the Information Age*, 2015 Wis. L. Rev. 321 (2015), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2615112
- Upturn, *Led Astray: Online Lead Generation and Payday Loans* (2015), https://www.upturn.org/reports/2015/led-astray/

FAMILY LAW

Technology impacts people's most personal relationships. This section highlights some areas family law attorneys for low-income families are likely to encounter in their practices, including predictive analytics in child welfare, technologically enabled abuses within intimate partner relationships, and the risk of data scraping of family court records, especially given that low-income families are more likely than wealthier ones to engage with court systems to resolve family disputes.

CHILD WELFARE

Jurisdictions in more than a dozen states have turned to predictive analytics to identify children at risk of abuse and neglect, and many more are considering adopting this algorithmic approach.[69] The stakes are high. Estimates are that 37% of children in the United States have caretakers who are investigated for child abuse and neglect by the time they turn 18.[70] Child protection agencies that fail to identify or ameliorate abuse or neglect can have dire consequences for children. At the same time, predicting risk where none exists can result in family separation, with traumatic impacts on parents and children. Given the stakes, along with the known biases of human decision-makers, predictive analytics holds the potential for more accurate and consistent interventions. However, as attorney Stephanie Glaberson states, "Unless careful attention is paid to the assumptions, biases, and realities of our child welfare system at this critical juncture, algorithmic decision-making risks perpetuating and magnifying existing problems."[71]

Predictive analytics in child welfare operate by analyzing information from multiple government data sets to generate a risk score assessing the likelihood of child

69 *See* Stephanie K. Glaberson, *Coding Over the Cracks: Predictive Analytics and Child Protection*, 46 Fordham Urb. L.J. 307, 331 (2019). Algorithms are also being used to recommend appropriate placement settings and match children with foster parents. *See* Devansh Saxena, *A Human-Centered Review of the Algorithms Used Within the U.S. Child Welfare System*, CHI '20 Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (Apr. 2020), https://www.shionguha.net/wp-content/uploads/2020/01/chi20c-sub2177-cam-i16.pdf.

70 Alexandra Chouldechova et al., *A Case Study of Algorithm-Assisted Decision Making in Child Maltreatment Hotline Screening Decisions*, 81 Proc. of Machine Learning 1 (2018), http://proceedings.mlr.press/v81/chouldechova18a/chouldechova18a.pdf.

71 Glaberson, *supra* note 69, at 310.

maltreatment. The scores are typically used to determine whether the agency will engage in further investigation and interventions. These scoring systems raise concerns around accuracy, fairness, and misuse. Faulty predictions can result from errors in data and algorithmic design. One national study found that agencies were struggling to obtain appropriate data for predictive systems.[72] Another study found "a lack of theoretically derived and validated algorithms that demonstrated that they took measures to integrate knowledge from the social sciences into their designs."[73]

With regard to fairness, there are concerns that algorithms will perpetuate the well-known patterns of race- and class-based discrimination in the child welfare system. These predictive analytics programs include data streams that disproportionately implicate poor people, such as receipt of public benefits and interactions in the criminal justice system. At the same time, these algorithmic analyses exclude the invisible data generated by the middle-class, who can gather support privately from therapists, doctors, private rehabilitation programs, and nannies and babysitters if they are struggling with mental health or addiction issues.[74] As Virginia Eubanks explains, this data never gets fed into child welfare algorithms.

By contrast, "Data that is ostensibly used to rate risk to child well-being can serve as a proxy for race or other past oppression, thereby over-representing those who have suffered from past marginalization as more risky,"[75] says Kelly Capatosto. Moreover, results can be misused when caseworkers overestimate their reliability or use results in unintended ways. Assessment scores may undermine the ability of caseworkers to rely on their professional judgment. Where a score suggests intervention, caseworkers may err on the side of family separation for fear of contradicting the algorithm. Further, the scores potentially divert attention away from providing families with needed social services that could alleviate the need to resort to family separation, such as family therapy, childcare assistance, or referral to substance abuse treatment.[76] In light of these problems, some jurisdictions have terminated their experiments with child welfare predictive analytics.[77]

Lawyers who work within the child welfare system can advocate for open, transparent processes around algorithmic adoption and contracting,[78] design, use, and evaluation.[79] They can use discovery processes such as interrogatories, document requests, and depositions to obtain information related to the application

72 Christopher Teixeira & Matthew Boyas, *Predictive Analytics in Child Welfare: An Assessment of Current Efforts, Challenges and Opportunities*, Prepared for the U.S. Dept. of Health & Human Svcs. (Oct. 2017), https://aspe.hhs.gov/system/files/pdf/257841/PACWAnAssessmentCurrentEffortsChallengesOpportunities.pdf.

73 Saxena, et al., *supra* note 69, at 8.

74 Virginia Eubanks, Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor 146–47, 156–57 (2017).

75 Kelly Capatosto, *Foretelling the Future: A Critical Perspective on the Use of Predictive Analytics in Child Welfare*, Kirwan Institute 4 (Feb. 2017), http://kirwaninstitute.osu.edu/wp-content/uploads/2017/05/ki-predictive-analytics.pdf.

76 *See* Clare Huntington, *The Empirical Turn in Family Law*, 118 Colum. L. Rev. 227, 299 (2018).

77 *See* Glaberson, *supra* note 69, at 335.

78 Christopher Teixeira et al., *Predictive Analytics in Child Welfare: Considerations in Contracting Vendors for Predictive Analytics*, Report for the U.S. Dept. of Health & Human Svcs. (April 2018), https://aspe.hhs.gov/pdf-report/predictive-analytics-child-welfare-considerations-contracting-vendors-predictive-analytics.

79 Saxena et al., *supra* note 69, at 6–8.

of algorithmic risk prediction tools in the case. Stakeholders[80] can advise on ethical issues,[81] as well as "when and how these tools can be used, what they can be used to model, what information they can access, who should have access to their scores or outcomes, and what individuals can do if they feel that erroneous information is utilized, their consent was not adequately sought, or they are treated unfairly as a result of the algorithm."[82] As one study concludes: "Given the limitations of predictive modeling methods, the ethical issues surrounding identification of families with a high-risk classification, and the potentially negative consequences of a false positive identification, model applications should be limited to preventive approaches and implemented if risk of unforeseen negative consequences is minimal."[83] In the future, we can expect that automated predictive systems will expand to other realms, such as to identify households at risk of elder abuse, and possibly to weigh the best interests of the child-in-custody determinations. It will be essential to apply the emerging lessons from the use of algorithms in the child welfare field to these new social service domains.

DOMESTIC VIOLENCE

New technologies raise several issues for domestic violence victims and their advocates, including how to handle coerced debt that becomes embedded in consumer reports, manage digital devices to maintain victims' safety, and respond to risk assessment tools. Coerced debt is a widespread problem for domestic violence victims. Professor Angela Littwin explains that it is a form of "financial abuse through consumer credit"[84] that involves "non-consensual, credit-related transactions that occur in an intimate relationship where one partner uses coercive control to dominate the other partner."[85] A study found that 52% of callers to the National Domestic Violence Hotline experienced coerced debt.[86] Coerced debt can involve an abuser applying for credit cards or other loans in a partner's name without their knowledge, as well as forcing a victim to obtain loans, buy items on credit for the abuser, or apply for public benefits. Both forms of coercion can result in debts in the victim's name and a damaged credit score. In cases of fraudulent debt, victims often do not discover the victimization until the debt is well into the collection process.[87] In turn, an adverse credit score limits access to housing,

80 Casey Family Programs, *Considering Implementing Predictive Analytics in Child Welfare* (Apr. 2018), https://caseyfamilypro-wpengine.netdna-ssl.com/media/Considerations-for-Applying-Predictive-Analytics-in-Child-Welfare.pdf.

81 Ravi Shroff, *Predictive Analytics for City Agencies: Lessons from Children's Services*, 5 Big Data 189 (2017), http://www.rshroff.com/uploads/6/2/3/5/62359383/predictive_analytics.pdf.

82 Glaberson, *supra* note 69, at 360.

83 Chris Scharenbroch et al., *Principles for Predictive Analytics in Child Welfare*, NCCD (Dec. 2017), https://www.nccdglobal.org/sites/default/files/inline-files/Principles%20for%20Predictive%20Analytics%20in%20Child%20Welfare-1.pdf.

84 Angela Littwin, *Coerced Debt: The Role of Consumer Credit in Domestic Violence*, 100 Cal. L. Rev. 951, 952 (2012).

85 Adrienne E. Adams, Angela K. Kittwin, & McKenzie Javorka, *The Frequency, Nature, and Effects of Coerced Debt Among a National Sample of Women Seeking Help for Intimate Partner Violence*, Violence Against Women (2019), at 2, https://journals.sagepub.com/doi/abs/10.1177/1077801219841445?journalCode=vawa.

86 *Id*. at 7.

87 *Id* at 11.

employment, utilities, a cell phone, and other needs—all of which can be essential to a victim seeking to build a life independent of their abuser.[88] These economic barriers can lead some victims to return to their abusers, or even discourage others from leaving their abusers in the first place. It also makes them vulnerable to predatory financial companies.[89]

There are steps that victims of coerced debt can take to clear their credit, although there are more remedies for victims of fraudulent debt (i.e., the victim did not know their identity was being used) than for coerced debt (i.e., the victim knew but acted under duress). Victims of fraudulent debt have the remedies under FCRA available to identity theft victims, as outlined above, such as disputing debt with CRAs, freezing credit, and putting fraud alerts on accounts. Some identity theft remedies hinge on filing a police report, which can be a problem for domestic violence victims who are wary of police involvement. Moreover, lawyers in some jurisdictions report that police are reluctant to issue reports in domestic violence situations.[90] Relatedly, there are also legal strategies for dealing with the consequences of coerced tax fraud and for defending against consumer collection actions. Regardless of the strategies taken to assist individual clients, all remedies must be considered with the victim's safety in mind. An essential resource for counseling victims of coerced debt and exploring legal remedies is by the Center for Survivor Advocacy and Justice.

With regard to coerced debt, remedies for victims are more complicated because consumer and family laws protect "innocent" third parties that extend credit, such as credit card companies. Legal reforms are necessary, including clarification that existing identity theft laws cover not only coerced debt linked to fraud but also debt generated by coercion, as Texas, New Hampshire, Massachusetts, and Ohio have done with their broader definitions of identity theft.[91] Reform is also needed with regard to legally recognizing economic abuse. The Violence Against Women Act (a federal law that funds antiviolence initiatives) and two-thirds of state laws do not recognize economic abuse as a form of domestic violence.[92] Even in jurisdictions where economic abuse is recognized as a harm, courts are limited in the corresponding remedies they can issue in a protection order.[93]

In addition to coerced debt, abusers can use various technologies to harass, impersonate, track, and control their victims by gaining access to texts, social media, emails, and smart home technology[94] and by placing geolocation trackers on cell phones and other devices. These tactics are called digital abuse, and

88 *Id.* at 12.

89 *See* Megan E. Adams, *Assuring Financial Stability for Survivors of Domestic Violence: A Judicial Remedy for Coerced Debt in New York's Family Courts*, 84 Brooklyn L. Rev. 1387, 1403–04 (2019).

90 *Id.* at 1393.

91 Ann Baddour & Marissa Jeffery, *Abuse by Credit: The Problem of Coerced Debt in Texas*, Texas Appleseed, http://stories.texasappleseed.org/abuse-by-credit-the-problem-of-coerced-debt-in-texas-.

92 Adams, *supra* note 89, at 1407.

93 *Id.*

94 Nellie Bowles, *Thermostats, Locks and Lights: Digital Tools of Domestic Abuse*, N.Y. Times (June 23, 2018), https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html; Karen Levy, *Intimate Surveillance*, 51 Idaho L. Rev. 679, 686–87 (2015).

it is experienced by 12% of people who have been in romantic relationships.[95] Technology can be used to relay threats, monitor a victim's movements and activities, steal passwords, and engage in public insults, among other harms.[96] Accordingly, victims may ask advocates for assistance in obtaining protective orders to stop digital abuse. They may also seek assistance in enhancing their online and device privacy.[97]

Technology is also being developed to prevent domestic violence and assist victims, although it will be essential to ensure that the tools are accurate and do not limit the victim's autonomy to seek the appropriate level of services that best meet their needs. Police departments and service providers have used risk assessments for many years to assess the victim's level of risk for future abuse. These assessments vary in their goals and content and some have limited empirical support.[98] Certain risk assessment tools focus on educating and empowering victims about their own safety and available options and resources; the empirical record with these tools is also mixed.[99]

Nevertheless, risk assessments are being digitized and integrated with machine learning and predictive systems[100] that pull from a wider array of data than was traditionally available, such as social media postings.[101] Other technologies under way include facial recognition and medical screenings that identify injuries consistent with domestic violence; monitoring devices for victims to wear that indicate when physical abuse is occurring; communication devices that allow victims to summon assistance; and apps that allow victims to assess their safety and connect them to resources. Other technologies are directed at monitoring abusers' whereabouts or predicting their likelihood of reoffending.[102] All of these emerging, automated systems raise issues of transparency, accuracy, and victim autonomy.

95 Michele Ybarra et al., *Intimate Partner Digital Abuse*, Data & Society (Jan. 18, 2017), https://datasociety.net/pubs/oh/Intimate_Partner_Digital_Abuse_2017.pdf.

96 National Network to End Domestic Violence, *A Glimpse from the Field: How Abusers are Misusing Technology* (2014), https://static1.squarespace.com/static/51dc541ce4b03ebab8c5c88c/t/54e3d1b6e4b08500fcb455a0/1424216502058/NNEDV_Glimpse+From+the+Field+-+2014.pdf.

97 Resources for the latter were developed at Cornell Tech and NYU and are available at this website: https://www.ipvtechresearch.org/resources.

98 *See* Emily Turner et al., *Dashing Hopes? The Predictive Accuracy of Domestic Abuse Risk Assessment by Police*, 59 British J. of Crim. 1013 (2019).

99 *See* Tara Richards et al., *An Examination of the Lethality Assessment Program (LAP): Perspectives on Implementation, Help-Seeking, and Victim Empowerment*, Violence Against Women (Oct. 29, 2019).

100 *See* Robin Petering, et al., *Artificial Intelligence to Predict Intimate Partner Violence Perpetration* (2018), https://www.researchgate.net/publication/329281099_Artificial_intelligence_to_predict_intimate_partner_violence_perpetration (predicting intimate partner violence among homeless youth).

101 *See* B. Chandramohan & T. Arunkumar, *Prediction and Prevention of Domestic Violence From Social Big Data Using Machine Learning Approach*, 120 Intl. J. of Pure & Applied Mathematics 3459 (2018), http://iab-rubric.org/papers/2018_CVPRW_PID5328687.pdf.

102 Richard Berk, et al., *Forecasting Domestic Violence: A Machine Learning Approach to Help Inform Arraignment Decisions*, 13 J. of Empirical Legal Studies 94 (2016).

"There can thus be a tension between the need to protect personal information and the need for aggregate data that can surface barriers to justice."

COURT RECORDS CONFIDENTIALITY

The privacy of information contained in courts records involving children and family relationships is a concern for litigants because court records are increasingly available online. The practical obscurity that maintained privacy in the paper-based era (i.e., requiring a trip to courthouse to pull a court file) has been replaced by digital open-access in many cases. This can make personally identifying information (such as names, phone numbers, emails, and addresses), along with sensitive information (financial disclosures, medical records, and relationship details), available to the general public as well as to the data broker industry.[103] The risks of public access to this information include identity theft, safety concerns (especially where domestic violence is involved), and digital profiling that includes highly sensitive information. At the same time, access to court data can be important for lawyers to engage in systemic overview and reform of judicial processes. There can thus be a tension between the need to protect personal information and the need for aggregate data that can surface barriers to justice.

Court records are presumed open under the First Amendment, although courts will balance this presumption against an individual's privacy rights. Matters involving family relationships tend to trigger the most protections for court records, although states vary widely in the types and extent of information protected. Generally, court records are publicly inaccessible in cases involving adoption, mental health, juvenile dependency, and termination of parent rights. Court records in other cases, including domestic violence, are generally publicly available. And juvenile records are surprisingly accessible electronically, creating serious collateral consequences in terms of education and jobs for people with records generated when they were minors.[104]

States will often protect certain records within family court files from public view, such as financial disclosure statements and medical records. In some jurisdictions, certain information may be available at the courthouse but not released on the internet. At a national level, the Violence Against Women Act prohibits internet access to identifying information in protective orders and restraining orders, but it does not prohibit in-person courthouse access. Other privacy provisions in state laws typically require the parties to take affirmative steps to request access restrictions, which can include redaction, sealing, and closed courtrooms. Thus, advocates need to know the open records laws in their jurisdiction and consider, with their clients, whether to seek additional protections where they are available—and perhaps to advocate for greater protections where they are not.

103 Erica McCrea, *A Survey of Privacy Protections in Guardianship Statutes and Court Rules*, 38 BIFOCAL 50 (2017), https://www.americanbar.org/groups/law_aging/publications/bifocal/vol_38/issue_3_february2017/privacy-guardianship.

104 Joy Radice, *The Juvenile Record Myth*, 106 Geo. L.J. 365, 385 (2018).

FAMILY LAW RESOURCES

- Megan E. Adams, *Assuring Financial Stability for Survivors of Domestic Violence: A Judicial Remedy for Coerced Debt in New York's Family Courts*, 84 Brooklyn L. Rev. 1387 (2019), https://brooklynworks.brooklaw.edu/cgi/viewcontent.cgi?article=2216&context=blr

- Stephanie K. Glaberson, *Coding Over the Cracks: Predictive Analytics and Child Protection*, 46 Fordham Urb. L.J. 307 (2019), https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=2757&context=ulj

- Rebecca Green, *Privacy and Domestic Violence in Court*, 16 Wm. & Mary J. Women & L. 237 (2010), https://scholarship.law.wm.edu/cgi/viewcontent.cgi?article=1054&context=wmjowl

- Emily Keddell, *Algorithmic Justice in Child Protection: Statistical Fairness, Social Justice and the Implications for Practice*, 8 Social Sciences 1 (2019), https://www.mdpi.com/2076-0760/8/10/281

- Michele Ybarra, Myeshia Price-Feeney, Amanda Lenhart, and Kathryn Zickuhr, Data & Society, *Intimate Partner Digital Abuse*, Jan. 18, 2017, https://datasociety.net/pubs/oh/Intimate_Partner_Digital_Abuse_2017.pdf

- Angela K. Littwin, *Coerced Debt: The Role of Consumer Credit in Domestic Violence*, 100 Cal. L. Rev. 1 (2012), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1867554

- Center for Survivor Agency and Justice, *CSAJ's Guidebook on Consumer & Economic Civil Legal Advocacy for Survivors* (2017), https://csaj.org/Guidebook

- National Center for State Courts, *Privacy/Public Access to Court Records*, https://www.ncsc.org/topics/access-and-fairness/privacy-public-access-to-court-records/state-links.aspx

- Texas Appleseed, *Coerced Debt Toolkit: Addressing Identity Theft for Survivors of Financial Abuse*, http://financialabusehelp.org/guide/coerced-debt-toolkit-overview

HOUSING

Major housing trends that impact low-income communities include the rise of "proptech" (property technology),[105] the digital management of the real estate industry, which manifests in digital applicant screening services, targeted advertising, new surveillance systems, and a booming short-term rental market. This section describes the trends impacting tenants, as well as issues around housing court record confidentiality.[106]

TENANT SCREENING

Across the United States, low-income people struggle to find affordable and habitable housing. One in three households struggles with housing costs that threaten their financial stability,[107] with a majority of low-income renters spending more than half their income on rent—and often much more.[108] While the rise of proptech promises frictionless property management for landlords, it raises potential pitfalls for tenants.

Landlords are increasingly screening potential tenants electronically in two ways. First, they are searching online eviction records made available through courts' case management systems. The problem with this method is that records used for case management purposes are not designed to give landlords the sort of information that would be meaningful in making a rental decision. They also tend to be plagued with inaccurate information, ranging from names and dates to dispositions and more. Moreover, court records will sometimes show that an eviction case was filed without listing the ultimate disposition of the case. Nevertheless, landlords often lack the context to

105 Erin McElroy, *Disruption at the Doorstep*, Urban Omnibus (Nov. 6, 2019), https://urbanomnibus.net/2019/11/disruption-at-the-doorstep.

106 Although this report focuses on tenants, low-income homeowners also face digital discrimination when data analytics rely on geographical data in advertising and lending practices and thereby reinforce inequalities of segregated housing markets. *See* Alex Rosenblat et al., *Data & Civil Rights: Housing Primer*, Data & Society (Oct. 30, 2014), https://datasociety.net/library/data-civil-rights-housing-primer; James A. Allen, *The Color of Algorithms: An Analysis and Proposed Research Agenda for Deterring Algorithmic Redlining*, 46 Fordham Urb. L.J. 219, 230–41 (2019).

107 Aspen Institute, Strong Foundations: Financial Security Starts with Affordable, Stable Housing (2020), https://assets.aspeninstitute.org/content/uploads/2020/01/Housing-Summary-Brief-1.pdf.

108 Matthew Desmond, Evicted: Poverty and Profit in the American City 2 (2016).

understand these limitations of court records. As a result, landlords tend to be overinclusive in screening applicants out of consideration.

Second, landlords are turning to tenant screening companies that score potential tenants across a variety of attributes, such as residential history, civil and criminal case history, and credit history. These reports include the inaccurate and misleading information gathered from court records, including a lack of case disposition.[109] They typically provide landlords with an applicant's "score" but don't include the underlying factors that lead to the score. Landlords will thus claim they are treating applicants equally because they do not know the underlying bases for those scores. These systems lack transparency, making it difficult to know whether the data analyzed by the algorithms is accurate, whether the algorithms select appropriate factors for inclusion, or how various factors are weighted. Without transparency, it is hard to hold any person or entity accountable for tenant screening decisions, even when they are unfair, inaccurate, or discriminatory.

Tenant advocates are working to bring transparency and accountability to this industry. For instance, a pending fair housing lawsuit is challenging a tenant screening company's algorithm.[110] In *Connecticut Fair Housing Center v. CoreLogic Rental Property Solutions, LLC,* a mother sought to have her disabled son move in with her, and she consented to a background check on her son's behalf. The tenant screening company used by the landlord determined that the son was disqualified from tenancy based on certain unspecified criminal

"Without transparency, it is hard to hold any person or entity accountable for tenant screening decisions, even when they are unfair, inaccurate, or discriminatory."

records. The son had been previously arrested, but not convicted, for theft, a charge that was withdrawn. In the lawsuit, plaintiffs assert that CoreLogic violated the Fair Housing Act by discriminating on the basis of race and national origin, given that criminal background records reflect disparities in the criminal justice system, and by offering a product that prevents landlords from conducting an individualized assessment of potential tenants. The federal district court dismissed the defendant's motion for summary judgment and ruled that the tenant screening company was covered by the Federal Housing Administration (FHA).[111] The case is proceeding.

Given that one-third of Americans possess a criminal record, the unrestrained use of criminal background screening in housing (and other domains) risks creating a permanent underclass of people unable to access basic life necessities. For this reason, in 2016, HUD issued *Guidance on Application of Fair Housing Act Standards to the Use of Criminal Records by Providers of Housing and Real Estate,* which discourages landlords from adopting automatic bans of applicants with criminal records and

109 *See* Lauren Kirchner & Matthew Goldstein, *Access Denied: Faulty Automated Background Checks Freeze Out Renters*, The Markup (May 28, 2020), https://themarkup.org/locked-out/2020/05/28/access-denied-faulty-automated-background-checks-freeze-out-renters.

110 Connecticut Fair Hous. Ctr. v. CoreLogic Rental Prop. Sols., LLC, 369 F. Supp. 3d 362, 372 (D. Conn. 2019).

111 *Id.* at 372.

instead recommends individualized determinations.[112] The incorporation of tenant eviction records into screening reports poses a similar problem;[113] such records are often incomplete and inaccurate and yet can permanently blacklist a tenant. As the founder of one tenant screening company told the *New York Times*, "No matter what the reason is and no matter what the outcome is (because) if their dispute has escalated to going to court, an owner will view them as a pain."[114] Low-income women of color are disproportionately impacted by tenant blacklists.[115] Tenant screening reports lack context: they do not necessarily show if the tenant won the case, if the tenant raised meritorious defenses, or if the case was dismissed.[116] And yet, regardless of fault or outcome, blacklisted tenants face ongoing struggles to find affordable and safe housing.

Landlords who impose automatic bans on tenants with eviction records likely violate the Fair Housing Act. A federal lawsuit against a landlord with such a policy was settled in 2017; under the settlement, the landlord rescinded the automatic ban, and tenants with eviction records can now obtain individualized review.[117] Of course, uncovering landlord policies around tenant screening reports may require lawyers or their clients to take affirmative steps to request FCRA reports. Under the FCRA, applicants for rental housing are entitled to information about a screening report that results in their denial of housing and to correct inaccurate information. In 2018, the FTC entered a $3 million settlement with a tenant screening company that failed to ensure its data was accurate.[118] It was found to have been carelessly matching people with similar names and birthdates to people with criminal records.

A few states and cities have enacted laws to blunt the effects of tenant blacklisting by sealing eviction records in certain circumstances, allowing eviction records to be expunged, regulating the content of tenant screening reports, or disallowing landlords to rely on publicly reported eviction data. Lawyers thus need to know what remedies are available in their jurisdiction to limit the harmful impacts of having an eviction case on a tenant's record. These remedies can be incomplete or difficult to enforce, particularly for the majority of tenants who lack legal counsel. Moreover, there are concerns that tenant screening companies are able to scrape data even from sealed or expunged cases. Nevertheless, these sorts of provisions are first steps

112 U.S. Dept. of Hous. & Urb. Dev., *Office of General Counsel Guidance on Application of Fair Housing Act Standards to the Use of Criminal Records by Providers of Housing and Real Estate-Related Transactions* (April 4, 2016), https://www.hud.gov/sites/documents/HUD_OGCGUIDAPPFHASTANDCR.PDF.

113 Housing Action Illinois & Lawyers' Committee for Better Housing, *Prejudged: The Stigma of Eviction Records* (March 2018), http://housingactionil.org/downloads/EvictionReport2018.pdf.

114 Teri Karush Rogers, *Only the Strongest Survive,* N.Y. Times (Nov. 26, 2006), https://www.nytimes.com/2006/11/26/realestate/26cov.html.

115 Sandra Park, *Unfair Eviction Screening Policies Are Disproportionately Blacklisting Black Women*, ACLU (Mar. 30, 2017), https://www.aclu.org/blog/womens-rights/violence-against-women/unfair-eviction-screening-policies-are-disproportionately.

116 Paula A. Franzese, *A Place to Call Home: Tenant Blacklisting and the Denial of Opportunity*, 45 Fordham Urb. L.J. 661, 669 (2018).

117 Nikita Smith v. Wasatch Property Management, Inc. et al., No 2:17-cv-00501 (W.D. Wash. March 30, 2017).

118 Lesley Fair, Federal Trade Comm'n, *$3 Million FCRA Settlement Puts Tenant Background Screening at the Forefront* (Oct. 17, 2018), https://www.ftc.gov/news-events/blogs/business-blog/2018/10/3-million-fcra-settlement-puts-tenant-background-screening.

toward securing housing for low-income people and provide models for expansion into other jurisdictions and/or federal legislation.

In sum, there are several mechanisms available to legal services lawyers who suspect or have evidence that their clients have been adversely impacted by a tenant screening report, including seeking the adverse action disclosures required under FCRA and state analogues; assessing federal and state fair housing claims for screening reports that discriminate intentionally on the basis of criminal or eviction records or that have a disparate impact on protected groups; and, depending on jurisdiction, enforcing (or advocating for) state and local laws that limit landlords' access to eviction records.

SURVEILLANCE

Surveillance tools, such as pervasive video cameras, are a fact of daily life for many low-income tenants. Some tenants welcome these systems for perceived security benefits; others are deeply concerned about the civil liberties implications of living under constant surveillance and the stigmatizing nature of tools that presuppose criminality. Tenant advocates are concerned that landlords are using selective portions of surveillance films as the basis for evictions, while tenants lack either access to the footage or the expertise to review thousands of hours of files if they can be obtained through discovery. In addition, some proptech tools require tenants to unlock their doors via smartphones, which some populations, such as the elderly, possess at much lower rates than the general population. Such systems can also pose safety and access challenges when there are power outages.

As a legal matter, challenging surveillance systems, whether they are public or private, is very difficult. The Fourth Amendment provides no restraint on government surveillance of public spaces,[119] and private landlords likewise can legally install cameras in any public, common area. While the Supreme Court has recently expressed concern about targeted surveillance tools,[120] there are no current constitutional restraints on the government's use of broad-based technology to monitor citizens. Further, there are no federal statutes restricting video surveillance in public spaces, although a few cities have adopted laws that regulate various surveillance tools within their jurisdiction.[121]

A growing form of surveillance is facial recognition technology, which uses algorithms to identify people by matching their image with those in existing databases, such as driver's licenses, arrest records, and social media. Over half of all Americans are in a facial recognition database, and those numbers are rising. Concerns about facial recognition include its lack of public knowledge or input; lower rates of accuracy for people of color, particularly women; the chilling effect on free speech; the lack of regulation; and the potential for law enforcement access without probable cause.[122] In the housing context, property managers are likely to deploy this technology to identify individuals who are barred from the property and to use their visits to it as grounds for eviction. This

119 "Given the low Fourth Amendment standards for stops, arrests, and searches in connection with minor misconduct, that outsized attention combines with the astounding array of conduct regulated in public and patrolled housing to permit police nearly unfettered authority." Alexis Karteron, *When Stop and Frisk Comes Home: Policing Public and Patrolled Housing*, 68 Case W. Res. L. Rev. 669 (2019).

120 Carpenter v. United States, 138 S. Ct. 2206 (2018).

121 *See* Ira S. Rubinstein, *Privacy Localism*, 93 Wash. L. Rev. 1961 (2018) (discussing surveillance ordinances in Seattle and New York City).

122 Clare Garvie & Laura M. Moy, *America Under Watch: Face Surveillance in the United States*, Georgetown Law Ctr. On Privacy & Tech (May 16, 2019), https://www.americaunderwatch.com.

is particularly problematic for domestic violence victims whose abusers are barred from the property but who may have little control over their abusers' visits.

In light of these and other concerns, some tenants are resisting facial recognition technology. A group of low-income tenants in Brooklyn, New York, filed a formal complaint with the state agency that oversees rent-stabilized properties after their landlord proposed replacing their keys with facial recognition technology. In the complaint,[123] filed by Brooklyn Legal Services, the tenants argued that the system was "an intrusion into the quiet enjoyment of their private home lives" and that the landlord could not establish that the system was necessary, accurate, or non biased. The landlord ultimately backed down from the plan.

The expansion of facial recognition technology has also spurred several cities and states to put moratoriums on the technology's use. Several cities have adopted laws limiting how facial recognition technology can be used by law enforcement and municipal agencies and requiring transparency around its adoption, deployment, and data usage. Some states are considering similar limitations, while a few states, including Illinois and Texas, already restrict commercial uses of biometric data. At the federal level, a proposed bill in 2019 would ban public housing authorities from adopting facial recognition technology. This is a fast-moving landscape of emerging laws; given the stakes for low-income people, legal services lawyers and their clients should be part of the discussions around proposed legislation.

AD DISCRIMINATION

Housing lawyers should be aware that their clients may be seeing—or not seeing—online housing ads tailored to their digital profiles. This is a form of digital redlining. In 2019, Facebook settled a lawsuit brought by numerous civil rights groups (including the National Fair Housing Alliance) alleging that its advertising platform allowed landlords and real estate brokers to target housing ads at specific populations while excluding people of color, families with children, women, people with disabilities, and other protected groups. Under the terms of the settlement,[124] Facebook agreed to terminate the ability of housing, employment, and credit advertisers to microtarget viewers based on protected characteristics or by zip code. HUD is pursuing a similar lawsuit.

However, ad delivery systems can replicate inequality through a variety of other mechanisms, including feeding people ads based on their browsing histories or those of their online connections. In turn, these ad delivery services can "reflect a prejudicial weblining effect and an adverse disparate impact on protected classes."[125] These ad delivery systems on internet platforms extend far beyond the realm of housing into lending, education, and other goods and services. Accordingly, poverty lawyers who suspect their clients are being denied online access to advertising information about housing opportunities should contact civil rights and/or fair housing organizations. It is also important to help clients identify alternate sources of information about housing opportunities.

123 In the Matter of The Owner's Application for Modification of Services, Tenants of Atlantic Plaza Towers, NYS Housing & Community Renewal Office of Rent Administration, Docket No. GS2100050D (Apr. 30, 2019), https://www.legalservicesnyc.org/storage/PDFs/%20opposition%20to%20facial%20recognition%20entry%20system%20app.pdf.

124 National Fair Housing Alliance, *Facebook Settlement: Civil Rights Advocates Settle Lawsuit with Facebook: Transforms Facebook's Platform Impacting Millions of Users* (2020), https://nationalfairhousing.org/facebook-settlement (linking to the plaintiff's complaint and the settlement agreement).

125 Rosenblat et al., *supra* note 109, at 5. *See also* Upturn, Leveling the Platform: Real Transparency for Paid Messages on Facebook (April 2018), https://www.upturn.org/static/reports/2018/facebook-ads/files/Upturn-Facebook-Ads-2018-05-08.pdf.

CONFIDENTIALITY OF HOUSING COURT RECORDS

As discussed above in connection with family law, court records in housing court can also contain a variety of sensitive information about litigants, including social security numbers, financial records, and sensitive medical and health information—the latter being a particular concern in supportive housing cases or in cases involving housing for disabled persons. As more court systems move to e-filing and online records maintenance, it is more likely that data brokers will scrape the data and include it in digital profiles, which may then be used in a discriminatory or unfair fashion. Open court records raise the risk of identity theft and other forms of fraud, as do court file data breaches. Balanced against these concerns are the American judicial system's commitment to open records.

State laws and policies around protecting privacy interests in court records vary widely and are shaped by First Amendment interests in access to information. Thus, it is essential for poverty lawyers to know the scope and scale of what court records are electronically available in their jurisdiction. For instance, some states allow bulk sales of court data to commercial buyers; a handful prohibit it. States vary in the types of data they automatically redact or permit parties to redact, such as financial information and social security numbers. Accordingly, once a lawyer understands what court records are publicly available in their jurisdiction, they should assess the tools that may be available to protect sensitive client information, such as sealing, redaction, protective orders, data minimization (putting less information on the official record), and stipulations.[126]

"As more court systems move to e-filing and online records maintenance, it is more likely that data brokers will scrape the data and include it in digital profiles, which may then be used in a discriminatory or unfair fashion."

Legal services lawyers should also demand a seat at the table when court systems evaluate and implement records access policies.

SHORT-TERM RENTAL PLATFORMS

The rise of short-term rental platforms, such as Airbnb, has mixed effects for low-income people. For some low-income homeowners, it provides a welcome stream of income support, although most property owners using rental platforms are white and wealthy. For renters, Airbnb is associated with decreases in affordable housing because it takes units off the long-term rental market, along with increases in average rents.[127] Short-term rental platforms also impact hotel workers, because the number of hotel stays decreases as short-term rentals increase. These platforms have been known to fight both the collection of occupancy taxes and compliance with zoning and health regulations. In light of these dynamics, housing advocates should be aware of the impacts of rental platforms in their

126 *See* Jeffrey W. Sheehan, *Confidences Worth Keeping: Rebalancing Legitimate Interests in Litigants' Private Information in an Era of Open-Access Courts*, 21 Vand. J. Ent. & Tech. L. 905 (2019), http://www.jetlaw.org/wp-content/uploads/2019/06/2_Sheehan_Final-3.pdf.

127 Josh Bivens, *The Economic Costs and Benefits of Airbnb*, Econ. Pol'y Inst. (Jan. 30, 2019), https://www.epi.org/publication/the-economic-costs-and-benefits-of-airbnb-no-reason-for-local-policymakers-to-let-airbnb-bypass-tax-or-regulatory-obligations.

jurisdictions and connect with impacted low-income homeowners and tenants to advocate for municipal policies that protect their interests.

HOUSING RESOURCES

- Esme Caramello and Nora Mahlberg, *Combating Tenant Blacklisting Based on Housing Court Records: A Survey of Approaches*, 2017 Clearinghouse Review 1 (2017), https://www.lcbh.org/resources/combating-tenant-blacklisting-based-housing-court-records

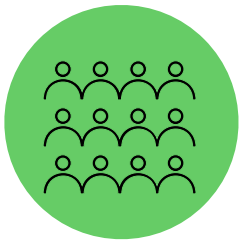
- *A Home of One's Own: The Fight Against Illegal Housing Discrimination Based on Criminal Convictions, and Those Who Are Still Left Behind*, 95 Texas L. Rev. 1103 (2017), http://texaslawreview.org/wp-content/uploads/2017/04/Crowell.pdf

- National Center for State Courts, *Privacy/Public Access to Court Records*, https://www.ncsc.org/Topics/Access-and-Fairness/Privacy-Public-Access-to-Court-Records/Resource-Guide.aspx

- Ariel Nelson, National Consumer Law Center, *Broken Records Redux: How Errors by Criminal Background Check Companies Continue to Harm Consumers Seeking Jobs and Housing*, Dec. 2019, https://www.nclc.org/images/pdf/criminal-justice/report-broken-records-redux.pdf

- Privacy Rights Clearinghouse, *The Renter's Guide to Tenant Privacy Rights*, https://privacyrights.org/consumer-guides/renters-guide-tenant-privacy-rights

PUBLIC BENEFITS



States are using algorithms to determine public benefits eligibility and identify supposed fraud in benefits receipt. Legal services attorneys who handle any form of government assistance, elder law, or health law will interact with these systems. Despite promises of increased efficiency and cost savings, automated decision-making systems tend to lack transparency and accountability and can be inaccurate and unfair, while denying many claimants their due process rights. Eubanks calls this shift toward automated systems the digital poorhouse, in which "surveillance and digital social sorting are driving us apart, targeting smaller and smaller microgroups for different kinds of aggression and control."[128] Philip Alston, the UN Special Rapporteur on extreme poverty and human rights, warns that we have entered a digital dystopia in which "systems of social protection and assistance are increasingly driven by digital data and technologies that are used to automate, predict, identify, surveil, detect, target and punish."[129] Professor Sarah Valentine states, "Big data analytics provides the state a degree of control over marginalized populations that is unrivaled in American history."[130]

There are thousands of horror stories of disabled and needy people being denied desperately needed state support due to an algorithmic eligibility determination.

"There are thousands of horror stories of disabled and needy people being denied desperately needed state support due to an algorithmic eligibility determination."

For instance, in 2016, Indiana entered a 10-year, $1.3 billion contract with IBM and a private call center company to automate its public benefits programs, including Medicaid and Supplemental Nutrition Assistance Program (SNAP). The algorithms employed to assess eligibility resulted in the denial of one million benefits in three years for "failure to cooperate"; this was an increase of 54% from the prior three years. IBM's system regularly lost claimants' records and verification documents, while penalizing people whose applications were missing documents or who made a mistake on a form (which could run to 120 pages). Thousands of people lost benefits, including a woman who missed a recertification phone call for Medicaid benefits because she was in the hospital being treated for ovarian cancer and was subsequently terminated for

128 Eubanks, *supra* note 74.

129 United Nations Human Rights Office of the High Commissioner, *World Stumbling Zombie-Like into a Digital Welfare Dystopia, Warns UN Human Rights Expert* (Oct. 27, 2019), https://www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=25156&LangID=E.

130 Sarah Valentine, *Impoverished Algorithms: Misguided Governments, Flawed Technologies, and Social Control*, 46 Fordham Urb. L.J. 364, 369 (2019), https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=2758&context=ulj.

noncompliance.[131] After three years, the state cancelled the contract and sued IBM. The Indiana Supreme Court eventually upheld a damages award to the state of $78 million.[132]

Problems with automated decision-making can arise from a variety of overlapping sources. To begin with, software developers must translate complex and often ambiguous regulatory requirements into computer code. Harmful errors have occurred in this transfer of lawmaking power to private vendors. Professor Danielle Citron explains that "programmers routinely change the substance of rules when translating them from human language into computer code."[133] She describes programmers in Colorado who, over three years, inaccurately translated at least nine hundred state regulatory requirements into code, leading to hundreds of thousands of erroneous decisions, including improper denials of health care to pregnant women, women with breast and cervical cancer, and foster children, as well as improper denials of food stamps to the disabled.[134] Such problems extend far beyond Colorado.[135] In addition to these translation errors, some of the algorithmic programs are simply wrong; they do not predict what they promise. Or they cannot handle outliers who do not fit the algorithm's preset parameters. Further, algorithms are fed data sets that often contain inaccurate or incomplete information. Meanwhile, some government agencies are purchasing algorithmic software without competitive bidding or public input, and they lack understanding of how algorithms work or the ongoing mechanisms for auditing and compliance monitoring.

Given this landscape, it's unsurprising that legal services lawyers have successfully challenged automated eligibility systems in several states and gained needed reforms. Courts have ruled that automated decisions that deny or reduce benefits without adequate notice or explanation deny constitutional due process rights to beneficiaries.[136] At the statutory level, courts have ruled that certain algorithms violate substantive requirements contained in laws and regulations.[137] In addition, the shift to automated decision-making can violate fundamental administrative law requirements, which in turn can be grounds for challenging algorithmic outcomes. When an agency secretly adopts algorithms that alter existing standards and processes, it can violate notice and comment requirements;[138] constitute arbitrary and capricious rulemaking; and result in administrative decisions lacking substantial evidence.

Cases that challenge algorithmic systems are complex and resource-intensive, and can require expert input and testimony. Indeed, says Valentine, "recent decisions reveal a judiciary that is struggling to grasp the technology and is relying on advocates to contextualize

131 Eubanks, *supra* note 74.

132 IBM Corp. v. Indiana, 124 N.E.3d 1187 (2019).

133 Citron, *Technological Due Process, supra* note 3, at 1254.

134 *Id.* at 1256, 1268–69.

135 *Id.* at 1270–71 (discussing similar errors in California and Texas); Valentine, *supra* note 133, at 372–73 (discussing public benefits problems in New York City and Michigan).

136 K.W. *ex rel.* D.W. v. Armstrong, 298 F.R.D. 479 (D. Idaho 2014).

137 *See* e.g., K.W. *ex rel.* D.W. v. Armstrong, 789 F.3d 962, 966 (9th Cir. 2015) (inadequate notice violated procedural due process and Medicaid requirements). *See also* cases collected in Valentine, *supra* note 133, at 415–16.

138 Ark. Dep't of Human Servs. v. Ledgerwood, 530 S.W.3d 336 (Ark. 2017).

system failures within the appropriate constitutional and statutory frameworks, be they criminal or civil."[139] In an individual case (as opposed to the class action and multi-plaintiff cases described above), lawyers litigating algorithmic determinations can raise many of the same arguments regarding procedural due process, substantive legal requirements, and administrative law standards.

Of course, litigation is not the only option for challenging algorithmic decision-making. Legal services lawyers have also successfully pressured legislators to engage in agency oversight and coordinated with the media to educate the public about the algorithmic deficiencies in these programs.[140] As a result, some jurisdictions have proposed or adopted laws designed to enhance algorithmic accountability. It is also essential for legal services lawyers and their clients to be at the table when government agencies decide to adopt new automated decision-making systems or replace legacy computer systems. Legal aid attorney Julia Simon-Mishel was involved as a stakeholder in a group overseeing Pennsylvania's adoption of a new unemployment insurance system. She describes a vendor's proposal to tag fraud when a benefits applicant lists the wrong employer from a pull-down menu. However, as Simon-Mishel pointed out to the stakeholder group, many employees only know the public-facing name of an employer and do not know the official name under which the employer is registered as a corporation. In turn, this could result in a wrongful denial of benefits or even the charge of fraud, which has its own collateral consequences. Without this insight into the perspective of claimants, the system might be designed to detect those innocent mistakes as fraud. Stakeholder input makes a difference.

As this example shows, states are using automated decision-making to ferret out alleged fraud in public benefits programs.[141] A high-profile system failure occurred in Michigan, which in 2013 automated its unemployment insurance benefits system with a $47 million program called Michigan Integrated Data Automated System (MiDAS) and laid off one-third of its workforce.[142] To identify fraud, MiDAS searched for discrepancies in recipients' records by cross-matching them with records from employers, other state agencies, and the federal government. Fraud determinations tripled to 40,000 in just two years—but 93% of them were wrong. How did MiDAS fail so spectacularly? Among the causes: the computer sent many notices to incorrect and dormant addresses; it issued vague notices; it could not distinguish between innocent mistakes and intentional fraud; it was designed to result in inadvertent admissions of fraud; and its process lacked recourse to human decision-makers. Upon a finding of fraud, the state demanded repayments plus interest and civil penalties of four times the amount owed; some assessments were as high as $187,000. To collect the funds, the state garnished wages, levied bank accounts, and intercepted tax refunds. The resulting financial stress resulted

139 Valentine, *supra* note 133, at 409.

140 Rashida Richardson, Jason M. Schultz, & Vincent M. Southerland, *Litigating Algorithms 2019 US Report: New Challenges to Government Use of Algorithmic Decision Systems* (AI Now Institute, Sept. 2019), https://ainowinstitute.org/litigatingalgorithms-2019-us.pdf.

141 *See* Michele Gilman, *AI Algorithms Intended to Root Out Welfare Fraud Often End Up Punishing the Poor Instead*, The Conversation (Feb. 14, 2020), https://theconversation.com/ai-algorithms-intended-to-root-out-welfare-fraud-often-end-up-punishing-the-poor-instead-131625; Stephanie Wykstra, *Government's Use of Algorithm Serves up False Fraud Charges*, Undark (June 1, 2020), https://undark.org/2020/06/01/michigan-unemployment-fraud-algorithm.

142 Cahoo v. SAS Analytics Inc., 912 F.3d 887, 892–93 (6th Cir. 2019). The court eventually approved a settlement in which the state agreed to cease operations.

in bankruptcies, damaged credit reports, evictions, homelessness, and even suicides. Litigation for damages to claimants continues.

Despite these cautionary tales, technological applications for identifying fraud are expanding. For instance, the Sacramento County (California) Department of Human Assistance entered into a contract with a private vendor that collects and stores license-plate reader data for use in investigating welfare fraud.[143] In light of these and other emerging technologies, poverty lawyers will need to stay attuned to state adoption of and changes to automated systems impacting eligibility and fraud determinations, including by monitoring public notice and comment rulemakings and funding bills where state agencies are seeking money to purchase new technologies. In addition, case surges with regard to particular benefits can signal adoption of new technologies. Lawyers will then need to advocate with state agencies to ensure that these systems are accurate, accountable, and transparent.

Public Benefits Resources

- Nicol Turner Lee, Paul Resnick, and Genie Barton, Brookings, *Algorithmic Bias Detection and Mitigation: Best Practices and Policies to Reduce Consumer Harms*, May 22, 2019, https://www.brookings.edu/research/algorithmic-bias-detection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms/
- Sarah Valentine, *Impoverished Algorithms: Misguided Governments, Flawed Technologies, and Social Control*, 46 Fordham Urb. L.J. 364, 409 (2019), https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=2758&context=ulj
- AI Now, *Litigating Algorithms 2019*, https://ainowinstitute.org/litigatingalgorithms-2019-us.pdf
- AI Now, *Algorithmic Accountability Policy Toolkit*, https://ainowinstitute.org/aap-toolkit.pdf

143 Dave Maass, *County Welfare Office Violated Accountability Rules While Surveilling Benefits Recipients*, Electronic Frontier Found. (July 31, 2018), https://www.eff.org/deeplinks/2018/07/county-welfare-office-violated-accountability-rules-while-surveilling-benefits.

SCHOOLS AND EDUCATION

Legal services lawyers who represent students and families in educational matters are most likely to see the impacts of technology in school surveillance and discipline in K–12 school systems, as well as predatory lending in the higher education sphere.

SURVEILLANCE AND SCHOOL DISCIPLINE

School systems are adopting new surveillance systems in the hopes of preventing school violence and identifying at-risk students for interventions.[144] Schools, particularly in minority communities, have long deployed security mechanisms generated within the criminal justice system, such as uniformed security officers, security cameras, metal detectors, and body searches.[145] A new repertoire of surveillance tools is layered on top of these methods, but these new tools are less visible. Companies sell these technologies to school districts as a means for predicting students' potentially harmful behavior. As a result, millions of students across the country are being monitored by surveillance systems that provide 24-hour analysis of words and phrases in students' social media accounts, chat messages, email, and schoolwork. These systems then alert school officials when they identify terms of concern. Professor Barbara Fedders explains, "The various mechanisms of surveillance combine to make more information available about more students, for a longer period of time, and accessible to a greater number of actors than was possible before the digital age."[146]

144 Schools are also using instructional technologies that allow private companies to mine student data for advertising and marketing purposes. *See* Barbara Fedders, *The Constant and Expanding Classroom: Surveillance in K-12 Public Schools*, 97 N.C. L. Rev. 1673, 1682–83 (2019). They are also using technologies to personalize education in ways that may entrench existing inequalities. *See* Andrea Alarcon et al., *Data & Civil Rights: Education Primer*, Data & Society (Oct. 30, 2014), https://datasociety.net/wp-content/uploads/2014/10/Education.pdf. While data mining is unlikely to be litigated in a civil legal services case, lawyers should be aware of how students' information is being gathered and processed in the event a client is involved in a school discipline case.

145 Jason P. Nance, *Implicit Racial Bias and Students' Fourth Amendment Rights*, 94 Ind. L.J. 47, 52–54 (2019).

146 Fedders, *supra* note 147, at 1675.

Some jurisdictions are using facial recognition technology to identify unauthorized visitors to school campuses. Another technology being promoted to schools is aggression detecting microphones, which their makers claim will identify anger in students' voices before tensions escalate.[147] The State of Florida is rolling out a system called the Florida Schools Safety Portal, which collects, aggregates, and analyzes data from school records, social services, and criminal records, along with public tips and social media scans, and makes the results available to law enforcement. [148]

School-based surveillance systems are generally legal under the Fourth Amendment; the governmental interest in reducing school crime is deemed to outweigh the privacy interests of students. Critics charge that school surveillance impinges the privacy and free speech rights of students in ways that can harm their creativity, social development, and educational outcomes; poses data security risks; and lacks empirical support for vendors' claims about improving student safety.[149] Most importantly for legal services lawyers who represent students in disciplinary hearings, these data-centric tools may also adversely and disproportionately impact minority students and students with disabilities.[150] Empirical evidence establishes that minority students are surveilled and punished for behavior at higher rates than similarly situated white students.[151]

These student populations are already at higher risk of entering the school-to-prison pipeline, the trend in which punitive school discipline policies, such as zero tolerance policies, shift children out of schools and into the criminal justice system. Issues that should be handled within families and communities become matters for law enforcement and state control. A study of one school district in Alabama found that 12-out-of-14 students expelled from school due to social media postings were African American, although African American students were only 40% of the district's population.[152]

147 Jack Gillum & Jeff Kao, *Aggression Detectors: The Unproven, Invasive Surveillance Technology Schools are Using to Monitor Students,* ProPublica (June 25, 2019), https://features.propublica.org/aggression-detector/the-unproven-invasive-surveillance-technology-schools-are-using-to-monitor-students.

148 *See* Anya Kamenetz & Jessica Bakeman, *To Prevent School Shootings, Districts Are Surveilling Students' Online Lives*, NPR (Sept. 12, 2019), https://www.npr.org/2019/09/12/752341188/when-school-safety-becomes-school-surveillance. A coalition of civil society groups wrote in opposition to the portal, in part because of potential harms on vulnerable groups. Valerie Strauss, *Civil Rights, Disabilities Groups Urge Florida to Stop Building Student Database They Call "Massive Surveillance Effort,"* Wash. Post (July 10, 2019), https://www.washingtonpost.com/education/2019/07/10/civil-rights-disabilities-groups-urge-florida-stop-building-student-database-they-call-massive-surveillance-effort.

149 *See* Fedders *supra* note 147, at 1702 ("the evidence of efficacy is scant; others have not been tested at all"); Benjamin Herold, *Schools are Deploying Massive Digital Surveillance Systems. The Results are Alarming*, Ed. Week (May 15, 2020), https://www.edweek.org/ew/articles/2019/05/30/schools-are-deploying-massive-digital-surveillance-systems.html.

150 *See* Priyam Madhukar, *The Hidden Costs of High-Tech Surveillance in Schools*, Brennan Ctr. for Justice (Oct. 17, 2019), https://www.brennancenter.org/our-work/analysis-opinion/hidden-costs-high-tech-surveillance-schools.

151 Nance, *Implicit Racial Bias*, *supra* note 148, at 72.

152 Sharada Jambulapati, *Story From the Field: Children of Color Pushed Out of Alabama Schools Over Social Media Posts*, Southern Poverty Law Center (July 9, 2015), https://www.splcenter.org/news/2015/07/09/story-field-children-color-pushed-out-alabama-schools-over-social-media-posts-0.

The predictive algorithms that underlie school surveillance, as well as their human analysts and adopters, may not understand the cultural vernacular of certain students, including immigrants, religious minorities, and students with disabilities. The risk is that the algorithm, and then school officials, will misinterpret innocent topics, slang, or jokes on social media as threats and push students into disciplinary proceedings and possibly involve law enforcement[153] In addition, school district officials are quick to scour for and punish sexualized language or imagery, even though such expressions are normal parts of normal adolescent development. Female students, particularly low-income girls of color, are particularly at risk of this form of surveillance. Accordingly, lawyers need to understand adolescent development in order to recognize normal behavior patterns and resist criminalizing frameworks.

In light of these trends, education lawyers will need to stay abreast of the surveillance technologies deployed in their jurisdiction and be attentive to any new patterns of school discipline, including among students with disabilities, who have special legal protections under the Individuals with Disabilities Act and Section 504 of the Rehabilitation Act for conduct related to their disabilities. While school discipline policies vary by state and locality, they all provide for some form of due process hearing before students are excluded from educational settings, and those hearings may also be sites for identifying and challenging surveillance tools.[154] Lawyers should ask for all evidence that the school is using against the student in a disciplinary proceeding. Under the Family Educational Rights and Privacy Act (FERPA),[155] parents have the right to inspect and view their child's educational records, including surveillance footage and other electronic evidence. A careful reading of FERPA and persistent advocacy are often necessary to obtain the evidence the school is using against a student.

Finally, and from a systemic perspective, under the Every Student Succeeds Act of 2015 (ESSA), school districts must publicly report the rates of suspensions, expulsions, school-related arrests, referrals to law enforcement, chronic absenteeism, and incidences of violence at the state, district, and school levels. This data may be helpful in understanding how new technologies are impacting school disciplinary practices and provide data for stakeholder input at the state and local level to support advocacy for reducing unfair and exclusionary discipline practices, such as through restorative justice programs and wraparound social services.

153 *Social Media Monitoring in K-12 Schools: Civil and Human Rights Concerns*, Ctr. for Democracy & Tech. & Brennan Center for Justice (Oct. 2019), https://www.brennancenter.org/sites/default/files/2019-10/CDT%20Brennan%20Statement%20on%20School%20Social%20Media%20Monitoring.pdf.

154 On defending students in school discipline proceedings, *see e.g.*, *School Discipline in New Jersey: A Toolkit for Students, Families, and Advocates*, Ed. Law Ctr. (2018), https://edlawcenter.org/assets/files/pdfs/publications/Student_discipline_manual.pdf; *The School Discipline Process: A Handbook for Maryland Families and Professionals*, Disability Rights Maryland (2015), https://disabilityrightsmd.org/wp-content/uploads/2017/08/Discipline-Manual.updated-July-2017.online-version.pdf; Talia Kraemer & Zabrina Aleguire, *Defending Students in Expulsion Proceedings: A Manual for Pro Bono Attorneys in CA*, Legal Services for Children (Dec. 21, 2015), https://www.lsc-sf.org/wp-content/uploads/2016/02/LSC-Expulsion-Defense-Manual.pdf.

155 20 U.S.C. § 1232g and 34 C.F.R. Pt. 99.

FOR-PROFIT COLLEGES

The for-profit higher education industry engages in predatory practices that target low-income students, people of color, single parents, older students, and veterans.[156] To enroll in for-profit colleges, students typically take out large, federally insured loans, yet these programs are of questionable quality and often do not result in the promised employment. One chain of for-profits investigated in 2017 by the California attorney general was charged with lying to students about job prospects, employing aggressive admissions counselors with rigid enrollment targets, saddling students with massive debt, and using unlawful debt collection practices.[157]

"To enroll in for-profit colleges, students typically take out large, federally insured loans, yet these programs are of questionable quality and often do not result in the promised employment."

Many potential students are targeted via lead generation.[158] Consumers who search online for terms related to education or employment ads are tagged by web browser cookies that track their online activity and allow for-profit colleges to follow them across the internet with targeted ads. When consumers fill out online forms posted by lead generators, their information is combined with other data about them to generate a score determining whether they are desirable targets. The Government Accountability Office conducted an investigation finding that within five minutes of entering a potential student's name and number into a single lead-generation site, the "student" received a recruiting call, followed by over 180 more calls within one month.[159]

Only 26% of students at for-profit colleges graduate within six years, as compared to 60% at public and private nonprofit schools. Even for those students who graduate, their job outcomes are actually worse than people with just a high school diploma.[160] Half of for-profit college students default on loans within five years of entering repayment, and there is no statute of limitations on collecting federal student debt. Although the Obama administration put in place regulations to

156 *See generally* Tressie McMillan Cottom, Lower Ed: The Troubling Rise of For-Profit Colleges in the New Economy (2017); Genevieve Bonadies, et al., *For-Profit Schools' Predatory Practices and Students of Color: A Mission to Enroll Rather than Education*, Harv. L. Rev. Blog (July 30, 2018), https://blog.harvardlawreview.org/for-profit-schools-predatory-practices-and-students-of-color-a-mission-to-enroll-rather-than-educate.

157 *See* Danielle Douglas-Gabriel, *California Attorney General Sues For-Profit Bridgepoint Education*, Wash. Post Nov. 29, 2017, https://www.washingtonpost.com/news/grade-point/wp/2017/11/29/california-attorney-general-sues-for-profit-bridgepoint-education.

158 Ctr. For Digital Democracy & U.S. PIRG, *Private For-Profit Colleges and Online Lead Generation: Private Universities Use Digital Marketing to Target Prospects, Including Veterans, via the Internet* (May 2015), https://uspirgedfund.org/reports/usf/private-profit-colleges-and-online-lead-generation.

159 U.S. Gov't Accountability Office, For-Profit Colleges: Undercover Testing Finds Colleges Encouraged Fraud and Engaged in Deceptive and Questionable Marketing Practices 15 (Aug. 4, 2010), https://www.gao.gov/assets/130/125197.pdf.

160 Stephanie Riegg Cellini & Nicholas Turner, *Gainfully Employed? Assessing the Employment and Earnings of For-Profit College Students Using Administrative Data* (NBER Working Paper Series May 2016), https://predatorystudentlending.org/wp-content/uploads/2018/03/2016_-_NBER_-_worse_off.pdf.

rein in industry abuses, these regulations have either been revoked or are in the process of being rescinded by the Department of Education, which is also halting numerous investigations into the for-profit education industry.[161] Future policies and enforcement will hinge on the commitments of the governing administration.[162]

In the face of these abuses, there are a variety of legal remedies, although they vary for public and private loans. Some states have relief programs (called state tuition recovery funds) for students victimized by predatory for-profit college conduct or school closures. There are also federal discharge programs that provide borrower defenses to repayment for school closures, although the Department of Education under Secretary Betsy DeVos has been gutting this defense, and litigation over the department's policies is ensuing. The Fair Debt Collection Practices Act (and state analogues) can protect against harassing and misleading debt collection practices,[163] and the TCPA can protect against certain debt collection robocalls to cell phones. The Equal Credit Opportunity Act has been the basis of lawsuits challenging discriminatory recruiting practices targeted at minorities. Students can also bring affirmative claims against schools that engaged in predatory conduct, as well as lenders and loan holders affiliated with the schools.[164] Students can also file complaints with state and federal agencies that oversee the industry.

EDUCATION RESOURCES

- Jessica Cardichon and Linda Darling-Hammond, *Protecting Students' Civil Rights: The Federal Role in School Discipline*, Learning Pol'y Inst., May 2019, https://learningpolicyinstitute.org/sites/default/files/product-files/Federal_Role_School_Discipline_REPORT.pdf
- Barbara Fedders, *The Constant and Expanding Classroom: Surveillance in K-12 Public Schools*, 97 N.C. L. Rev. 1673 (2019), https://scholarship.law.unc.edu/cgi/viewcontent.cgi?article=6749&context=nclr
- Dignity in Schools Campaign, NAACP Legal Defense and Educational Fund Inc., and Partners for Each and Every Child, *Engage for Education Equity: A Toolkit for School Communities on the Every Student Succeeds Act*, https://www.naacpldf.org/wp-content/uploads/EfEE_Full-Toolkit.pdf
- Melissa Frydman and Shani King, *School Discipline 101: Students' Due Process Rights in Expulsion Hearings*, Clearinghouse Review 370 (Sept.-Oct. 2006), https://www.law.ufl.edu/_pdf/about/faculty/SMKClearinghouseReviewArticle.pdf
- Alyssa Rafa, *The Status of School Discipline in State Policy*, Education Commission of the States, Jan. 2019, https://www.ecs.org/wp-content/uploads/The-Status-of-School-Discipline-in-State-Policy.pdf
- Project on Predatory Student Lending, https://predatorystudentlending.org/about-the-project/
- National Center on Safe Supportive Learning Environments, *School Discipline Laws & Regulations by State*, https://safesupportivelearning.ed.gov/school-discipline-laws-regulations-state

161 Bonadies et al., *supra* note 160.

162 There are multiple policy reforms that would protect students, see Robert Shireman, *The Policies That Work – and Don't Work – to Stop Predatory For-Profit Colleges*, The Century Foundation (May 20, 2019), https://production-tcf.imgix.net/app/uploads/2019/05/20105707/Shireman_9policies_FinalPDF1.pdf.

163 State claims may be particularly important in light of FDCPA exemptions for creditors, servicers, and government agencies; however, there are federal preemption issues. National Consumer Law Center, Student Loan Law 14.2.4.2 (6th ed. 2019), updated at https://www.nclc.org/library.

164 *Id.* at Ch. 14.

WORKERS' RIGHTS

Technology is reshaping the American workplace, with some adverse impacts on low-wage workers who may seek legal representation to learn and assert their rights. This section covers workplace legal problems typically handled by legal services offices, such as digital wage theft, automated scheduling and hiring systems, and worker monitoring. Unemployment insurance is another key issue for worker advocates as states replace their legacy systems with machine learning systems for eligibility and fraud detection; it is addressed in the "Public Benefits" section of this report.

DIGITAL WAGE THEFT

Low-wage workers have long suffered from wage theft, that is, the failure to be paid for work performed. Studies show the amount of wage theft is over $15 billion per year.[165] A rising scourge is digital wage theft, which results from timekeeping software used for hourly employees, who constitute almost 60% of the American workforce.[166] Instead of the punch cards of yore, employees now log their time through computers, smartphones, RFID badges, and iris recognition devices, and in turn this information is electronically transmitted to timekeeping software.[167] At first glance, this software might seem far more accurate and foolproof than records kept by hand. However, some automated timekeeping software allows employers to edit down hours worked, automatically round arrival and departure times to a preset increment that shaves off time worked, and impose automatic break deductions, which assume the worker took the full break allowed, even if work conditions made that impossible (a common problem for health care providers).

Professor Elizabeth Tippett analyzed hundreds of cases of digital wage theft, including one case in which the use of rounding software caused 2,100 casino workers to lose a combined 87,710 hours over five

165 David Cooper & Teresa Kroeger, *Employers Steal Billions From Workers' Paychecks Each Year*, Economic Policy Institute (May 10, 2017), https://www.epi.org/publication/employers-steal-billions-from-workers-paychecks-each-year.

166 Elizabeth C. Tippett, *How Timekeeping Software Helps Companies Nickel and Dime Their Workers*, The Conversation, Jan. 11, 2017), https://theconversation.com/how-timekeeping-software-helps-companies-nickel-and-dime-their-workers-70981.

167 Elizabeth Tippett, Charlotte S. Alexander & Zev Eigen, *When Timekeeping Software Undermines Compliance*, 19 Yale J.L. & Tech. 1 (2018).

"A rising scourge is digital wage theft, which results from time-keeping software used for hourly employees, who constitute almost 60% of the American workforce."

years, amounting to nearly $950,000 at their $10.80 hourly wage. Unfortunately, existing regulations governing timekeeping were written over 50 years ago, during an era when time was kept by hand and exact precision was not realistic, and thus they permit the practice of rounding. As a result, workers challenging these practices have the burden to prove that the rounding practices do not average out in the long term. Yet, timekeeping software is programmed to favor employers so that averaging out is no longer a sound presumption. Additionally, employees lack the knowledge to understand how their time is counted, creating an information asymmetry.

Workers challenging digital wage theft have remedies under the federal Fair Labor Standards Act (FLSA),[168] as well as state and local wage and hour laws. Although the FLSA's recordkeeping requirements aren't enforceable in a private action, workers can enforce the act's substantive requirements. FLSA requires covered employers to pay a minimum wage for each hour worked and an overtime wage for time worked over 40 hours. Remedies for wage theft can include back wages and hefty penalties. Unfortunately, collecting on wage judgments from some employers can be extremely challenging, as they may change addresses, dissolve their company, and otherwise hide assets. As a result, some states allow workers to put a lien on employer assets before or at the time a complaint is filed.

Further, depending on the state and its commitment to enforcing its wage laws, workers may find assistance enforcing their rights from state labor agencies, and in some jurisdictions, criminal prosecutors are charging employers with wage theft.[169] Due to the technological transformations in timekeeping, advocates need to be familiar with how timekeeping software operates and to know the full range of enforcement and recovery options in their jurisdiction.

UNPREDICTABLE SCHEDULING

Unpredictable scheduling is a major problem in the low-wage workforce. Many employers use just-in-time software that allows them to schedule shifts with little notice in order to reduce wage costs and manage staffing levels. However, for workers, erratic scheduling make planning budgets, childcare, family obligations, medical appointments, education, and other jobs challenging and stressful.

Accordingly, several states and jurisdictions—including Vermont, Oregon, New York City, San Francisco, Chicago, Philadelphia, and Seattle—have passed predictive scheduling laws, also called fair workweek laws. Laws vary, but they generally cover retail, hospitality, and fast food workers; and typical provisions include requiring advance notice of schedules, extra pay for scheduling changes, guarantee of minimum shifts, and rest periods between shifts. By contrast, some states— such as Arkansas, Georgia, Iowa, and Tennessee—have laws forbidding their counties and cities from passing employment-related laws, which is a way to preempt fair workweek laws in those states.

Legal services lawyers in jurisdictions with fair workweek laws may handle compliance issues as employers adjust to (or attempt to evade) the new

168 U.S. Dept. of Labor, Wages and the Fair Labor Standards Act, https://www.dol.gov/agencies/whd/flsa.

169 Chris Opfer, *Prosecutors Treating "Wage Theft" as a Crime in These States*, Bloomberg Law (June 26, 2018), https://news.bloomberglaw.com/daily-labor-report/prosecutors-treating-wage-theft-as-a-crime-in-these-states.

standards. In places lacking fair workweek legal protections, advocates may want to join or support coalitions advocating for adoption of such laws.

AUTOMATED HIRING

Employers are increasingly using predictive decision-making tools to hire workers. The technology enables them to determine where to post jobs and what audiences to target, screen qualified candidates, and conduct preemployment assessments. In addition, new technologies are being used to conduct automated video interviews. Applicants are then scored based on analysis of their facial expressions, tone of voice, conversational content, and other factors.[170] Software vendors have touted these various tools for their efficiency, cost-effectiveness, and lack of prejudice, which can bedevil human interactions.[171]

However, privacy and employment advocates have cautioned that these technologies can replicate existing structural biases in society because they are trained on datasets that include the embedded biases of prior generations.[172] For instance, Amazon tested, and subsequently abandoned, an algorithm to hire employees that was based on the prior 10 years of résumés of successful company hires.[173] Because those hires were predominately male due to the gender imbalance within the tech industry, the algorithm consistently recommended men over women. Similar examples of algorithms replicating gender and racial biases abound throughout workplace hiring systems. Relatedly, various online personality tests, used heavily by employers in the low-wage workforce, inquire about or attempt to assess the applicant's mental health, which in turn can result in disability discrimination.[174] While legal services lawyers generally do not handle employment discrimination cases, they may become aware of systemic problems within their client populations and be well situated to refer cases to civil rights attorneys.

"...these technologies can replicate existing structural biases in society because they are trained on datasets that include the embedded biases of prior generations."

In addition, legal services lawyers may work with clients who are struggling to obtain employment because employers are rejecting them owing to information in their digital profiles. Background checks typically include credit history, past employment, and information from public records, including criminal records. Background checks can include computer-generated predictions based on unreliable information

170 Illinois passed a law requiring notice, consent, deletion rights, and an explanation to applicants if they are using AI for video interviews. Other states may follow suit. *See* Rebecca Heilweil, *Illinois Says You Should Know if AI is Grading Your Online Job Interviews*, Vox Recode (Jan. 1, 2020), https://www.vox.com/recode/2020/1/1/21043000/artificial-intelligence-job-applications-illinios-video-interivew-act.

171 *See* Miranda Bogen, *All the Ways Hiring Algorithms Can Introduce Bias*, Harvard Bus. Rev. (May 6, 2019), https://hbr.org/2019/05/all-the-ways-hiring-algorithms-can-introduce-bias.

172 *See* Pauline Kim, *Manipulating Opportunity*, 106 Va. L. Rev. 867 (2020).

173 Jeffrey Dastin, *Amazon Scraps Secret AI Recruiting Tool That Showed Bias Against Women*, Reuters (Oct. 9, 2018), https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G.

174 *See* Matthew T. Bodie, Miriam A. Cherry, Marcia L. McCormick, & Jintong Tang, *The Law and Policy of People Analytics*, 88 U. Colo. L. Rev. 961, 980–85 (2017).

and questionable inferences. For instance, Upturn writes about a background check vendor that flags candidates it deems at risk of engaging in sexual harassment and other toxic workplace behavior based on social media posts and other public online content.[175] According to a 2018 survey, 95% of employers are conducting background screening, and 94% of those include a form of criminal history check.[176] There are approximately 2,000 background screening companies; the three largest conduct over 50 million checks a year.[177]

Criminal background checks are deeply problematic given their unreliability and lack of proven connection to job performance. Between 70 and 100 million Americans have criminal records, which can serve as a barrier to employment. Errors can arise when background check companies do not update court records, thereby reporting expunged or dropped cases, or fail to state a case's final disposition. In addition, the reports often contain data belonging to a different person; data that is over seven years old and thus banned under FCRA; and multiple versions of the same charges, giving the false impression of a lengthier criminal history. While applicants can review and correct their credit reports with the big three credit reporting agencies, that remedy is difficult to pursue for background checks, given that there are over 2,000 background screening companies.[178]

For all these reasons, as of 2019, 35 states and more than 150 cities and counties have enacted ban-the-box laws that forbid employers from asking about criminal history until later in the hiring process, when there is greater opportunity for an individualized assessment. As noted in the "Consumer Law" section of this report, FCRA applies to employers using consumer reports in employment decisions, as well as the companies that generate the reports (despite attempts by many data brokers to evade coverage). Employers must tell applicants they are conducting a background check, obtain written consent, provide a pre-adverse action notice with a copy of the consumer report and notice of rights under FCRA, and a final notice of rights once the denial is final. Individuals have the ability to challenge the content of the report, although as noted earlier, these processes can be time-consuming.

Some employers will access social media and court records themselves, without relying on an outside company. In these cases, FCRA does not apply, and remedies are few. However, a handful of states bar employers from accessing social media accounts.

EMPLOYEE MONITORING AND SURVEILLANCE

Surveillance and monitoring pervade the low-wage workplace. Employers routinely require personality and drug tests before hiring and throughout employment; they observe workers through video cameras, monitor computer keystrokes, listen to telephone calls, review emails and internet usage, and track movements through GPS or radio frequency devices. Employers use an array of algorithmic management tools "to remotely manage workforces, relying on data collection and

175 Miranda Bogen & Aaron Rieke, *Help Wanted: An Examination of Hiring Algorithms, Equity, and Bias*, Upturn 39 (Dec. 2018).

176 Consumer Financial Protection Bureau, Market Snapshot: Background Screening Reports (Oct. 2019), https://files.consumerfinance.gov/f/documents/201909_cfpb_market-snapshot-background-screening_report.pdf.

177 Ariel Nelson, *Fertile Ground for FCRA Claims: Employee & Tenant Background Checks*, National Consumer Law Center (Dec. 16, 2019), https://library.nclc.org/fertile-ground-fcra-claims-employee-tenant-background-checks

178 *Id.*

surveillance of workers to enable automated or semi-automated decision-making."[179] Worker performance is quantified through continual data collection, which puts pressure on workers that can compromise their safety, increase their stress, and result in disciplinary actions.[180] These surveillance and monitoring systems lack transparency, obscure power imbalances between employers and workers, and make it difficult for workers to negotiate for better conditions.[181]

Nevertheless, there are few legal protections against employer surveillance and monitoring tools. No federal law limits worker surveillance. Most states prohibit surveillance in highly intimate settings (such as locker rooms and bathrooms) but otherwise, employers have few restraints on watching their employees. Most employees are at-will, and employers can condition employment on consent to a variety of monitoring practices. Unionized workers are sometimes able to bargain for surveillance limits in their contracts, but only 10.3% of the workforce is unionized.[182] Regardless of union membership, the National Labor Relations Act protects employees who communicate, including on social media and in emails, about their working conditions.

Other legal protections from surveillance are scattered and narrow and vary by state. For instance, some states prohibit employers from demanding access to employees' social media, and some prohibit employers from tracking employees. Overall, the law provides little privacy protections for workers, but lawyers should be familiar with the available workplace protections in their jurisdiction and consider organizing and advocacy strategies to meet the privacy needs of workers.

MISCLASSIFICATION

Related to wage theft is misclassification of workers as independent contractors rather than employees. When workers are misclassified as independent contractors, they can find themselves underpaid because they lack the overtime and minimum wage protections of employees. In addition, independent contractors do not receive employment benefits or antidiscrimination protections, they do not have the right to collectively bargain, and they are not covered by unemployment insurance, workers compensation, or occupational health and safety laws. Moreover, these employers and their workers do not contribute to social insurance programs and employment taxes, thus reducing funding overall.[183] Technology has digitized the scourge of misclassification. Gig workers perform on-demand service work arranged over web-based platforms, such as "chauffeur driving, food and goods delivery, home cleaning, gardening, and errand-running."[184] A Federal Reserve study puts the number of gig workers at 75 million. In addition to the lack of protections afforded

179 Alexandra Mateescu & Aiha Nguyen, *Explainer: Workplace Monitoring & Surveillance*, Data & Society (Feb. 6, 2019), https://datasociety.net/library/explainer-workplace-monitoring-surveillance.

180 Julia Ticona, Alexandra Mateescu & Alex Rosenblat, *Beyond Disruption: How Tech Shapes Labor Across Domestic Work & Ridehailing*, Data & Society (June 2018), https://datasociety.net/wp-content/uploads/2018/06/Data_Society_Beyond_Disruption_FINAL.pdf.

181 Mateescu & Nguyen, *supra* note 179.

182 Bureau of Labor Statistics, Union Members 2019 (Jan. 22, 2019), https://www.bls.gov/news.release/pdf/union2.pdf.

183 *See* David Weil, *Lots of Employees Get Misclassified as Contractors. Here's Why It Matters*, Harv. Bus. Rev. (July 5, 2017), https://hbr.org/2017/07/lots-of-employees-get-misclassified-as-contractors-heres-why-it-matters.

184 Veena B. Dubal, *Winning the Battle, Losing the War?: Assessing the Impact of Misclassification Litigation on Workers in the Gig Economy*, 2017 Wis. L. Rev. 239 (2017).

employees, gig workers also face the risk of being fined for breaching user agreements because they stand in the role of consumer vis-à-vis the internet platform on which they obtain work.

The law is still sorting through how to treat these workers. In general, the line between an employee and independent contractor hinges on the level of control the employer has over the worker—greater control is indicative of employment status. As Professor Veena Dubal states, "On the one hand, [gig] workers are encouraged to act entrepreneurially and through self-initiative to make money for themselves and the firm. On the other hand, many of these firms claim that software is their core competency, and thus workers performing tasks and services through the software have been 'externalized' as independent contractors."[185] There have been numerous lawsuits challenging the classification of gig workers as independent contractors, but as Professor Miriam Cherry explains, "No clear consensus has emerged on how the courts will determine employee versus independent contractor status for workers in the on-demand economy. Many of the cases that might have provided important rulings have settled."[186]

Lawmakers are also wading in to resolve the issue. Arizona, Florida, Indiana, Iowa, Kentucky, Tennessee, Texas, Utah, and other states have codified on-demand gig workers as independent contractors. By contrast, California passed a statute in 2019 that significantly reduces the ability of employers to classify gig workers as independent contractors, and other states, such as New Jersey, Illinois, and New York, are considering similar legislation. Uber, Lyft, and other platform businesses have announced that they will not comply with the California statute and intend to defend their position in litigation. They are also funding a ballot initiative to exempt them from the law. Suffice to say, classification issues for workers in the platform economy are an unsettled issue that will be disputed in coming years. Advocates for low-wage workers will need to stay abreast of these developments and use litigation and law reform strategies to ensure that workers whose employment terms are controlled by their employers are classified as employees.

185 *Id.* at 75–51.

186 Miriam A. Cherry, *Beyond Misclassification: The Digital Transformation of Work*, 37 Comp. Lab. L. & Pol'y J. 577 (2016).

WORKERS' RIGHTS RESOURCES

- Ifeoma Ajunwa, Kate Crawford, and Jason Schultz, *Limitless Worker Surveillance*, 105 Cal. L, Rev. 735 (2017), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2746211
- Miranda Bogen & Aaron Rieke, *Help Wanted: An Examination of Hiring Algorithms, Equity, and Bias*, Upturn 39 (Dec. 2018).
- Miriam A. Cherry, *Beyond Misclassification: The Digital Transformation of Work*, Comp. Labor L. & Pol'y J. (2016), https://scholarship.law.slu.edu/cgi/viewcontent.cgi?article=1009&context=faculty
- Veena B. Dubal, *Winning the Battle, Losing the War?: Assessing the Impact of Misclassification Litigation on Workers in the Gig Economy*, 2017 Wis. L. Rev. 239 (2017), https://repository.uchastings.edu/cgi/viewcontent.cgi?article=2597&context=faculty_scholarship
- Alexandra Mateescu and Aiha Nguyen, Data & Society, *Explainer: Workplace Monitoring & Surveillance*, Feb. 6, 2019, https://datasociety.net/output/explainer-workplace-monitoring-surveillance/
- Alexandra Mateescu and Aiha Nguyen, Data & Society, *Explainer: Algorithmic Management in the Workplace*, Feb. 6, 2019, https://datasociety.net/output/explainer-algorithmic-management-in-the-workplace/
- Julia Ticona, Alexandra Mateescu, and Alex Rosenblat, Data & Society, *Beyond Disruption: How Tech Shapes Labor Across Domestic Work & Ridehailing*, June 26, 2019, https://datasociety.net/output/beyond-disruption/
- Elizabeth Tippett and Charlotte S. Alexander, *When Timekeeping Software Undermines Compliance*, 19 Yale J.L. & Tech. 1 (2017), https://yjolt.org/when-timekeeping-software-undermines-compliance
- The Center for Popular Democracy, *A Practice Guide to Combatting Wage Theft: Lessons from the Field*, Nov. 2017, https://populardemocracy.org/sites/default/files/WTHandbook-web_output%20%281%29.pdf
- Fair Workweek Initiative, http://www.fairworkweek.org/policy-innovations

IMMIGRATION SURVEILLANCE

The United States has built a massive, technologically fueled immigration surveillance system that has expanded aggressively in recent years. The National Immigration Law Center explains, "Immigrants are caught in a complex and opaque web of databases, related systems, and information-sharing mechanisms that facilitate immigration enforcement and erect barriers to their full participation in economic and social life in the United States."[187] A full description of immigration surveillance and the legal tools to constrain these systems are outside the scope of this report and are available elsewhere. Nevertheless, this section provides a brief overview of immigration surveillance because legal services lawyers who represent immigrants on other civil matters should be aware of the ways in which their clients are being tracked for purposes of immigration enforcement.

Federal agencies are engaged in extensive data sharing with state and local law enforcement and licensing agencies. For example, a local police department can take fingerprints at the scene of an arrest and run them against FBI and Department of Homeland Security (DHS) databases, which in turn generate a notice to Immigration and Customs Enforcement (ICE) if there is a match so that ICE can arrange to have the person held until it can pick them up. The data matching goes both ways; ICE and the FBI have access to state and local criminal justice records, along with certain states' facial recognition technology, which is typically generated from driver's license records.[188] The federal government is also deploying automated license-plate readers to record license plates and track drivers' movements and social media monitoring of visa applicants and immigrants, including legal permanent residents and naturalized citizens.[189] In addition, ICE has contracts with private data brokers to conduct continuous monitoring of personal data, including credit history, utility records, cell phone accounts, driver's license information, public court records, employment address data, and criminal records. Put together, "this amounts to a moment-by-moment monitoring of immigrant activities during the lifecycle of their interactions with the United States, as opposed to the previous system of checkpoint-based immigration enforcement."[190]

187 *Untangling the Immigration Enforcement Web: Basic Information for Advocates about Databases and Information-sharing Among Federal, State, and Local Agencies*, National Imm. L. Ctr. (Sept. 2017), https://www.nilc.org/wp-content/uploads/2017/09/Untangling-Immigration-Enforcement-Web-2017-09.pdf.

188 *Face Recognition and Driver's License Photo-Sharing*, National Imm. L. Ctr. (Oct. 2019), https://www.nilc.org/issues/drivers-licenses/face-recognition-and-dl-photo-sharing.

189 Joan Friedland, *Information Vacuuming: The Trump Administration is Collecting Massive Amounts of Data for its Immigrant Surveillance and Deportation Machine*, National Imm. L. Ctr. (Aug. 22, 2018), https://www.nilc.org/2018/08/22/information-vacuuming-immigrants-and-citizens.

190 Chinmayi Sharma, *The National Vetting Enterprise: Artificial Intelligence and Immigration Enforcement*, Lawfare (Jan. 8, 2019), https://www.lawfareblog.com/national-vetting-enterprise-artificial-intelligence-and-immigration-enforcement.

While there are few legal limits on immigration surveillance, some states and jurisdictions are declaring themselves sanctuaries and resisting coordination with federal immigration enforcement efforts. Civil rights and immigration lawyers have used constitutional claims to fight back against surveillance that results in national origin profiling and raised Fourth Amendment defenses against warrantless searches. These are ongoing and urgent efforts. For civil legal services lawyers who do not practice immigration law, questions about immigration surveillance are likely to surface, such as the risks of an undocumented person filing a wage claim or housing court case. Accordingly, these issues may require coordination with and education from immigration lawyers within a specific jurisdiction to fully counsel clients about the risks and benefits of asserting various rights in civil forums.

IMMIGRATION RESOURCES

- Joan Friedland, National Immigration Law Center, *Information Vacuuming: The Trump Administration Is Collecting Massive Amounts of Data for Its Immigrant Surveillance and Deportation Machine*, Aug. 22, 2018, https://www.nilc.org/2018/08/22/information-vacuuming-immigrants-and-citizens/

- Brennan Center for Justice, *Social Media Surveillance by Homeland Security Investigations: A Threat to Immigrant Communities and Free Expression*, Nov. 15, 2019, https://www.brennancenter.org/our-work/research-reports/social-media-surveillance-homeland-security-investigations-threat

- Electronic Frontier Foundation, *Immigrant Surveillance*, https://www.eff.org/tags/immigrant-surveillance

- Anil Kalhan, *Immigration Surveillance*, 74 Md. L. Rev. 1 (2014). National Immigration Project, https://www.nationalimmigrationproject.org/index.html

- National Immigration Law Center, *Untangling the Immigration Enforcement Web: Basic Information for Advocates about Databases and Information-Sharing Among Federal, State, and Local Agencies*, Sept. 2017, https://www.nilc.org/wp-content/uploads/2017/09/Untangling-Immigration-Enforcement-Web-2017-09.pdf

CONCLUSION

Data-centric technologies impact everyone in the United States. However, the impacts can be particularly harmful to people without economic resources, who are disproportionately people of color. Every day, legal services lawyers assist low-income clients in meeting their basic needs, such as housing, food, education, employment, medical care, and family stability. This report suggests four broad lessons for these lawyers, who are on the frontlines in identifying and challenging emerging technologies that are adversely impacting clients.

First, low-income people and their lawyers must be at the table when governments are considering adopting automated decision-making systems and then remain engaged in ongoing oversight. Their insights can improve the accuracy and ethical use of these systems. Legal services lawyers and their clients also have a tremendous amount of information and experience to share with policymakers who are considering new laws related to data privacy and protection. It is essential that emerging laws protect the interests of all persons, not just those of elites and industry. Next, legal services lawyers need additional training and funding to understand and interrogate algorithmic systems and challenge them in court. This is the time for technologists working toward digital justice to join with legal services lawyers to share and build on each other's expertise. Finally, many of the remedies suggested in this report are challenging for a high-volume legal services office to pursue; these offices must often triage their clients' most urgent needs. The issues highlighted this report, then, are ideal for partnering with, or referrals to, law offices or pro bono lawyers who engage in impact litigation. In the fight for access to justice, poverty lawyers and their clients need to expand their toolbox—but the tools are within reach.

ACKNOWLEDGEMENTS

This report was made possible with the generous time and insights of the following legal experts: Erica Braudy, New York Legal Services; Jordan Brensinger, Columbia University; David Brody, Lawyers' Committee for Civil Rights; Louise Carwell, Legal Aid Bureau of Maryland; Ana Cisneros Alvarez, Wage Justice Center; Catherine Cramer, Northeast Big Data Hub; Hilary Dalin, Office of Elder Justice and Protective Services; Sharon Dietrich, Community Legal Services of Philadelphia; Eric Dunn, National Housing Law Project; Elizabeth Edwards, National Health Law Program; Jennifer Egan, Maryland Office of the Public Defender; Professor Barbara Fedders, University of North Carolina School of Law; Alyssa Fieo, University of Baltimore School of Law; Stevie Glaberson, Public Justice; Cornelia Bright-Gordon, Legal Aid Bureau of Maryland; Jon Greenbaum, Lawyers' Committee for Civil Rights; Alex Gulotta, Komenge Law; Kevin de Liban, Legal Aid of Arkansas; Office of New York City Councilwoman Helen Rosenthal; Carla Leticia Sanchez-Adams, Texas RioGrande Legal Aid, Inc., Jeffrey Senter, Legal Aid Society, Harlem Community Law Office; Julia Simon-Mishel, Philadelphia Legal Assistance; Angela Tripp, Michigan Legal Help Program; David Udell, National Center for Access to Justice; Elizabeth Wells, Silicon Valley Legal Foundation; Judith Whiting, Community Service Society; Morgan Williams, National Fair Housing Alliance; and Chi Chi Wu, National Consumer Law Center. In addition, the clinical faculty at the University of Baltimore School of Law provided valuable feedback: Professors Katy Clemens, Daniel Hatcher, Margaret Johnson, Neha Lall, Jaime Lee, Hugh McClean, Nicole McConlogue, Nickole Miller, Jane Murphy, Colin Starger, Alexandra Smith, and Shanta Trivedi. Finally, a big thanks to the teams at Data & Society for supporting this work and helping make this report a reality.

RECOMMENDED READING LIST

The following books provide in-depth explorations of the mechanics and impact of data-centric technologies on low-income people, people of color, and other marginalized groups:

- Ruha Benjamin, *Race After Technology: Abolitionist Tools for the New Jim Code* (2019)
- Meredith Broussard, *Artificial Unintelligence: How Computers Misunderstand the World* (2018)
- Sasha Costanza-Chock, *Design Justice: Community-Led Practices to Build the Worlds We Need* (2020)
- Catherine D'Ignazio and Lauren F. Klein, *Data Feminism* (2020)
- Virginia Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor* (2019)
- Safiya Umoja Noble, *Algorithms of Oppression: How Search Engines Reinforce Racism* (2018)
- Cathy O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* (2016)
- Frank Pasquale, *The Black Box Society* (2015)
- Alex Rosenblat, *Uberland: How Algorithms Are Rewriting the Rules of Work* (2018)
- Sara Wachter-Boettcher, *Technically Wrong: Sexist Apps, Biased Algorithms, and Other Threats of Toxic Tech* (2017)

Data & Society is an independent nonprofit research institute that advances new frames for understanding the implications of data-centric and automated technology. We conduct research and build the field of actors to ensure that knowledge guides debate, decision-making, and technical choices.

www.datasociety.net
@datasociety

Designed by Yichi Liu

DATA&
SOCIETY

www.datasociety.net

@datasociety