RIGHTS & SECURITY INTERNATIONAL

Dangerous Data

Police Abuse of Access to Personal Data in the United States and its Global Implications

APRIL 2026

privacyinternational.org

rightsandsecurity.org

ABOUT PRIVACY INTERNATIONAL

Governments and corporations are using technology to exploit us. Their abuses of power threaten our freedoms and the very things that make us human. That's why Privacy International campaigns for the progress we all deserve. We're here to protect democracy, defend people's dignity, and demand accountability from the powerful institutions who breach public trust. After all, privacy is precious to every one of us, whether you're seeking asylum, fighting corruption, or searching for health advice. So, join our global movement today and fight for what really matters: our freedom to be human.

ABOUT RIGHTS & SECURITY INTERNATIONAL

Rights & Security International (RSI) works to halt human rights abuses that governments commit in the name of national security. Founded in 1990 to promote justice for abuses during the armed conflict in Northern Ireland, our organisation now works internationally to promote the freedoms of expression, belief and association, while continuing to tackle harms such as torture, arbitrary detention, enforced disappearance and discrimination. Based on rigorous fact-finding, we advocate for better laws and policies, and help build movements for change.

Privacy International
62 Britton Street, London EC1M 5UY,
United Kingdom
privacyinternational.org

Privacy International is a registered charity (1147471), and a company limited by guarantee registered in England and Wales (04354366).

Rights & Security International
465c Hornsey Road, London N19 4DR,
United Kingdom
rightsandsecurity.org

Rights & Security International is a registered charity (1048335), and a company limited by liability (companies house number 2489161)

Contents

Back to Contents ↑

I. Introduction and Summary

In the United States today, police officers can stalk, needlessly detain, wrongly arrest, and even injure and kill people as a consequence of warrantless searches of vast collections of personal data.

These databases sprang from post-9/11 government decisions to amass or gain access to information about millions of people whom the authorities did not suspect of any wrongdoing – and from a private data broker industry that caters to the government's desire to be able to "connect the dots."

Today, this government impulse to create or buy access to collections of personal data about extremely large numbers of people, and give law enforcement access to those databases, is not restricted to the US: for example, the UK, in 2024, adopted laws that would give authorities access to bulk collections of data from social media. However, the results of such practices in the US should serve as a global warning: law enforcement access to large collections of personal data, without a warrant, is dangerous for the public and even for fellow officers.

Police officers are human, and giving them warrantless access to large collections of data about people results in entirely foreseeable harms.

While the media and the public are increasingly alert to the dangers of police use of artificial intelligence (AI), our research shows that serious problems can arise before the government or a data company applies AI software to a large collection of personal data. Warrantless access to such databases can result in human rights violations, including racial injustice and gender-based violence, even if the eye-catching issue of AI never comes into play.

In the years immediately after 9/11, US federal government decisions to create "Total Information Awareness" about ordinary people were intensely controversial. Today, however, they have become the new normal: sprawling government-run and private-sector databases that put masses of information about ordinary people at officers' fingertips have left the realm of counter-terrorism (where they can be a threat to human rights as well) to become a ubiquitous tool of everyday policing.

Under US law, the databases and warrantless police access to them are currently legal: there are no constitutional bars to their existence or their use by law enforcement, and few restrictions under statutory law. As a result, the private sector has developed systems that it markets specifically and openly to police, and law enforcement bodies have also created their own sprawling databases of personal information about individuals. Given a broad political trend of supporting wider policing powers and declining to impose curbs, as well as the profit motive of the private sector, these practices appear highly likely to continue.

Worsening the situation for individuals, under current US federal laws and most if not all state laws, there are no requirements for these records about people to be correct. They do not have to be necessary for any given purpose. Known mistakes do not need to be fixed. And the systems are available to regular officers both at their desks and in their vehicles, nationwide.

The result is an evisceration of the human right to privacy, as well as foreseeable mistakes and abuses by officers. Our research indicates that those mistakes and abuses particularly harm women and (other) people of color – as well as police themselves, when officers decide to target their own colleagues. It also prompts questions about whether inaccurate database information may sometimes underlie US police raids on wrong addresses (including under "no-knock warrants"), which can have deadly consequences.

These harms have occurred throughout the country and across multiple presidential administrations; because they appear to arise from gaps in the law and a lack of accountability, we see no reason to believe they will abate if the political climate in the country changes—unless much stronger protections are adopted and enforced.

While our research draws on evidence from the US, police abuse of access to personal data could become an issue in many countries around the world, including regions such as the UK and the EU that have been adopting greater data access powers for law enforcement. We highlight the serious consequences of unrestrained police access to government or private databases through examples from US federal cases, and call for legislatures everywhere to investigate such practices in their jurisdictions – and impose necessary safeguards against abuse.

For this report, we examined judicial opinions and other records from 130 federal civil lawsuits filed since 2011 (a time when such suits were gradually becoming more common) that provided evidence of police misuse of large digital collections of personal information. Although US media outlets have previously reported on some aspects of police access to, and misuse of, government databases, this report uniquely provides an in-depth examination of this number and range of federal civil rights lawsuits. Wherever possible, we have relied on statements of fact that were agreed between the parties, testimony given by the defendants, jury verdicts, or similar sources, rather than allegations that were not accepted by either the defendants or the court. The cases we examined span a majority of US states.

Among the cases our report describes are those in which the agreed facts suggest, or the plaintiffs have offered evidence to support an argument, that:

- Police have relied on inaccurate information in databases to make wrongful arrests, leading to the detention and prosecution of innocent people.

- Even when the database information is correct, police have used personal information in government and private-sector databases in abusive, negligent or otherwise harmful ways, also leading to wrongful arrests and other damaging consequences. For example, US police currently have the legal power to look up the personal data of passing or parked cars without any fact-based suspicion of wrongdoing, a situation that has contributed to harmful encounters between police and innocent people (particularly Black Americans).

- Police can and do look up personal information about women without any law enforcement justification, including – at times – with the intention of engaging in stalking and sexual abuse.

- Police have improperly – and at times illegally – looked up information about their fellow officers, justice professionals, and public safety personnel, including current and former female colleagues.

Many of the cases we discuss resulted in profound and lasting consequences for people who were the subject of warrantless lookups, and in some instances their family members. Some of the cases described below include those brought by:

- Nathaniel Maybin, Jr., who was arrested in Philadelphia for an armed assault he did not commit and detained in jail for more than 17 months.
- A South Carolina woman known in court as Jane Doe, whom a police officer looked up and allegedly sexually assaulted – resulting in a $500,000 jury verdict against the authorities.
- The mother of Burrell Ramsey-White, a bystander in a Boston neighborhood where someone had reported a man looking into car windows. Police chased and ultimately shot Ramsey-White, who died shortly afterward.
- Karl Augustus, who became a target for police simply for driving a "nice" car in Los Angeles' Skid Row and was surrounded by officers with their guns drawn – and a helicopter – after a database search wrongly led the police to conclude that the car might be stolen.
- A woman we are calling H.W., who was legally blind and a stroke survivor, and whom police handcuffed and detained in Maryland although she had done nothing wrong.
- Alix Kendall, a Minnesota TV news broadcaster, who learned that police officers and other government employees throughout the state had secretly looked up her driver's license information – including her picture – nearly 4,000 times.

In each of these cases, the ability of US police to search for personal data in large databases without a warrant or court order contributed – or directly led – to serious harms. In the absence of strong limitations on when and how officers can look up and use personal information, people in any country will experience similar threats to their rights.

These episodes have damaging consequences: in addition to the immediate harms such as being detained or jailed, people at the receiving end of these bad practices have highlighted long-term anxiety and other psychological distress as well as harms to family and professional life. Several people who brought court actions have described lasting harms to their dignity, including feelings of humiliation and – in a disturbing and common theme – having been "violated." Some, such as those mistakenly arrested, continue to be linked with derogatory information appearing in online search results.

As a further cautionary note to governments, the absence of strong protections against police access to, and misuse of, personal data in the United States has also led to municipalities paying millions of taxpayer dollars in settlements and damages to alleged victims. These large, avoidable expenditures of public funds have occurred even though many and perhaps most federal civil rights lawsuits in these cases that have reached the judgment phase – that is, cases that did not end early due to settlements – have resulted in a finding that the police were entitled to "qualified immunity," meaning that they were not legally liable for the harms done.

Under international human rights law, governments – including police departments – are obligated to respect the right to private life. This means not gathering, storing, or viewing information in a manner that interferes with people's privacy unless such activities are carried out on the basis of clear legal authorizations that impose limits to protect rights, are done in pursuit of a legitimate aim, and are necessary to achieving that aim. Even if the way a data broker or another government agency originally obtained information about someone was lawful, human rights norms do not then grant police carte blanche to view that data or buy access to it: such activities must still be necessary to achieving a legitimate aim, non-arbitrary, and done in accordance with a clear authorization in law.

Human rights courts and experts also increasingly recognize that people are entitled to a baseline set of rights protections when a government or business gathers or processes personal data about them, regardless of whether the data itself has implications for privacy as such. Moreover, the UN's top human rights agency has opined that the human right to privacy continues to apply in public spaces and to information that someone has publicly shared (for example, on social media websites).[1]

Yet, in the US, private-sector databases (especially) offer a startling range of information: they may incorporate race, physical description, and biometric data; social media, financial, and location data; records about vehicles and gun licenses; educational and employment information; and links between individuals, their family members and purported "associates" and family members – leading people to become potential subjects of police investigations simply because (according to the database) someone they know has been arrested or convicted in the past. Government-run databases, too, can include large amounts of data about individuals, including (for example) arrests that never led to convictions.

While the rapid and easy accessibility of law enforcement databases (whether government-run or operated by the private sector) may intuitively appear to bolster police efficiency, and potentially increase officers' safety, the ubiquitous access described in this report creates identifiable dangers. For example, in a harsh irony, some people become crime victims when police misuse these databases to – for example –look up and then stalk women. We also identify a risk that people will stop calling police during emergencies for fear that police will look up and then arrest the caller or bystanders, as has occurred in reality.

Despite many challenges, victims and alleged victims of police misuse of personal data have continued to fight for justice – even though suing police departments can be costly, time consuming, and intimidating.

1 UN Office of the High Commissioner for Human Rights, "The right to privacy in the digital age," U.N. Doc. A/HRC/39/29, August 3, 2018, ¶ 6.

To prevent police misuse of large collections of personal data, we recommend that the US establish in federal law that people have a privacy interest in data that can be linked to them as identifiable individuals; end the amassing of personal data in bulk; require an individualized court order based on a specific statutory authorization for all law enforcement collection and storage of personal data; and require the government to monitor the accuracy of, and delete, personal data it holds that is outdated, incorrect, or no longer strictly necessary to achieving a legitimate aim.

The US should also restrict the types of personal information private companies can collect, store and sell (or donate); create a legal basis for suing police who access personal data without authorization; and take other steps to ensure the accuracy and protection of personal information available to law enforcement.

At the most basic level, this report establishes that people in authority can and will abuse their access to personal data if few or no strong deterrents stand in their way. In our interpretation of the facts, those abuses can be racist or misogynist, and are sometimes so severe as to be deadly or lead to injury. Personal data is never "just data," and governments should legislate accordingly.

Lastly, although our research largely did not address immigration enforcement in the United States and was drafted before the highly visible immigration arrests and deportations that have occurred under the second Trump administration, we encourage readers to consider what warrantless access to massive (and potentially inaccurate) collections of data about individuals and families might mean for immigration enforcement.

Back to Contents ↑

II. Methodology

The main research for this report took place at various times from May 2018 to September 2024, with interruptions due to the COVID-19 pandemic and other factors. The main sources for the investigation included open-source research using thousands of pages of US federal court records, private companies' marketing materials, and other evidence concerning databases.

Outside of the EU, international human rights law sources discuss but typically do not define the term "personal data" when describing rights obligations or assessing harms. For the purposes of this report, we have adopted the approach found in the EU's GDPR, which defines "personal data" as including "any information relating to an identified or identifiable natural person" (and establishes protections for this data).[2] While not all such data may appear to be inherently sensitive, it is susceptible to misuse or mishandling that violates privacy, non-discrimination, or other rights, as the GDPR implicitly recognizes – and as this report shows.[3]

Our research focused on searchable electronic databases of stored personal information that government authorities in the US maintain for, or that companies market to, law enforcement. This report therefore does not directly address law enforcement's ability to search for personal information using search engines or social media websites available to the general public, such as Google or Facebook, although publicly posted information from social media sites may be aggregated and stored in the databases we have addressed. Some intelligence agencies refer to government searches of social media sites as "social media intelligence," or SOCMINT—another growing and problematic practice that human rights organizations such as ours believe is not subject to sufficient safeguards.[4]

The goals of our research were to determine whether US legal protections for personal data are sufficient to prevent police misuse of the information, identify common harms among the cases we examined, document those harms, and make recommendations for reforms accordingly. We complemented this research with an analysis of the global data broker industry, to understand where the data in these databases may originate. We also performed a comparative analysis of the legal protections that exist in the EU to prevent police misuse of personal data, to identify useful provisions that could be replicated elsewhere as well as those that would need to be reinforced.

To find the pool of cases, we searched for judicial opinions in US federal lawsuits using privately owned databases of US court decisions, which are widely used in the US legal sector. (We note that these databases share corporate relationships with some of the private-sector products for law enforcement that are mentioned in this report; unfortunately, few if any comparable products from other sources are available.) We used combinations of keywords such as "law enforcement," "database," and "qualified immunity" (a US legal term describing officers' immunity from lawsuits under a range of circumstances) to find cases involving claims of civil rights abuses by police in which databases were involved.

---

2 European Union, Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, April 27, 2016, art. 4(1).

3 See, e.g., ibid., recitals 71 and 75.

4 See, e.g., Privacy International, "Social media monitoring in the UK: the invisible surveillance tool increasingly deployed by the government," July 17, 2024, https://privacyinternational.org/long-read/5337/social-media-monitoring-uk-invisible-surveillance-tool-increasingly-deployed (accessed September 17, 2025); *Privacy International*, "How your social media activity is monitored by the police", March 11, 2019, . https://privacyinternational.org/long-read/2722/how-your-social-media-activity-monitored-police (accessed September 17, 2025).

After identifying such cases, we examined them in more detail using the Public Access to Court Electronic Records (PACER) database. Focusing on federal court cases – which, unlike state cases, are compiled in a single, accessible online location – provided an efficient means of locating evidence, judges' discussions of alleged facts, and the authorities' responses to claims of civil rights violations. This approach also allowed us to assess whether victims of illegal, unnecessary, or otherwise problematic police searches of data have access to adequate redress for harms.

Several dozen of these cases, chosen to illustrate common problems we identified, are specifically described in this report. While our methodology did not enable us to make statistical findings, the number and nature of the cases we located allowed us to find and analyze common themes.

We supplemented this research into civil cases with available information from media reporting, several criminal prosecutions of officers who had allegedly misused their database access, academic analyses, and other sources.

Although this report focuses on several problematic patterns of police conduct identified through the search methods described above, other problems that can result from the misuse of databases or incomplete records – such as the mistaken detention of US citizens for immigration enforcement purposes – have been the subject of reporting elsewhere.[5]

Civil lawsuits in the United States concerning alleged rights violations often do not result in a published judicial opinion until months or even years after the events in question. The violations and alleged violations described in this report therefore span an unusually long period – from 2007 to 2021 – while any harms allegedly committed more recently had not yet resulted in published opinions or other adequate records that were available to us when we were conducting the research. However, the patterns of mistakes and misconduct we have identified are sufficiently persistent that we believe the risk of harms remains the same today.

In many of the cases described below, police officers or departments disputed at least some of the facts alleged by the plaintiff or prosecutor. Wherever possible, this report relies on factual claims that were uncontested or that a court has presented as sufficiently plausible (or agreed) to form a basis for decision-making at the pre-trial stages of the case. In many of our discussions, we have drawn on courts' decisions on motions for summary judgment; parties (typically defendants) often make such motions in US federal court at the pre-trial stage, arguing that the judge should decide the case in their favor by simply applying the law to what is known about the case, because there is no "genuine dispute as to material fact."[6] When ruling on such motions, judges sometimes simply recite what the plaintiff has alleged, and sometimes delve into the evidence (usually by looking at what the defendants have admitted).

---

5 See, e.g., Sam Biddle, "ICE Searched LexisNexis Database Over 1 Million Times in Just Seven Months," *Intercept,* June 9, 2022, https://theintercept.com/2022/06/09/ice-lexisnexis-mass-surveillances/ (accessed September 17, 2025); Paige St. John and Joel Rubin, "Must Reads: ICE held an American man in custody for 1,273 days. He's not the only one who had to prove his citizenship," *Los Angeles Times*, April 27, 2018, (accessed August 28, 2019). https://www.latimes.com/local/lanow/la-me-citizens-ice-20180427-htmlstory.html (accessed September 17, 2025).

6 Federal Rules of Civil Procedure, Rule 56, available at https://www.law.cornell.edu/rules/frcp/rule_56.

The reader should be aware that when making decisions on motions for summary judgment, federal judges will construe the evidence in the light most favorable to the party that did not make the motion.[7] In the cases described below, this usually means the court would have presented the available evidence in the light most favorable to the plaintiffs—that is, the people who said their constitutional rights had been violated. We have therefore looked carefully at the facts asserted in each case and what evidence the court cited when describing them. When we describe a claim that the other party disputed, and regarding which the judge did not give some indication that the court viewed the claim as credible based on the information available in the record, we have striven to note the dispute in the text or footnotes. While we have taken great care to avoid relying on the plaintiffs' allegations alone, the reader should be aware of the potential for human error in this respect.

For descriptions of the databases, we have largely drawn on marketing materials and other documents published by private companies that sell database access to law enforcement, as well as materials published or distributed by government agencies. Where appropriate, we requested comments from the companies mentioned in this report; we only received a response from Spokeo, which we have summarized below.

This report's main drafter also interviewed 17 academic, civil-society, and other experts for this report, and attempted to contact the plaintiffs' legal representatives from many of the civil cases described below. Seven plaintiffs or their attorneys spoke with us on the record, and the plaintiffs were specifically informed that they could decline to answer questions, or terminate the interview, at any time. Attorneys for an eighth plaintiff invited the main drafter to observe the 2019 federal jury trial in what remains one of the few lawsuits we have examined that has successfully reached such a stage; during the eight-day trial, the drafter observed testimony by Amy Krekelberg (see below) and her police colleagues, among others. Where academic and other experts were concerned, a particular effort was made to consult with women, who have historically been underrepresented in published scholarship on data and technology.

Due to the passage of time, we have chosen not to quote these interviews, with the exceptions of one with an attorney who has since passed away. The other interviews have informed our conclusions, and we are grateful to all interviewees for contributing their thoughts, especially those who described the physical and emotional impacts of their experiences with data misuse. We also especially note the valuable and ever-increasing contributions of women scholars and lawyers, and those of color, to the field and urge that fellow attorneys, journalists, data privacy experts and others consult with (and quote or cite) these experts routinely.

We have used initials instead of full names for plaintiffs in this report where a court has previously granted anonymity, the case involved sensitive circumstances such as allegations of gender-based violence, or our case descriptions include health information. Where appropriate, we have withheld identifying information about such cases in our citations; however, for all cases, we retain the relevant records on file or are able to access them in PACER.

7 Ibid.

Back to Contents ↑

III. Background

A.
Scant laws lead to big data

In the modern United States, it is virtually impossible to avoid generating personal data that is then recorded and stored in an electronic database simply by living one's everyday life. Births, marriages, divorces, deaths, court cases, and interactions with police result in government records, while ordinary activities such as obtaining home electricity from a power company or ordering items online generate data that the private sector can share or sell.

Legal protections have failed to keep pace with these developments, and as a result of this failure and other factors, police in the US now have widespread access to digitized and sometimes highly revealing – or inaccurate – personal data from large databases compiled by the government or private companies.

i. "Collect it all": The growth of police and private-sector data-gathering

a. Government data collection for law enforcement takes off

Since the attacks of September 11, 2001, US intelligence and law enforcement agencies have often depicted the gathering and sharing of personal information as essential to preventing "terrorism" (a term that remains undefined in international law) and other violence.[8] Nearly 18 years after the attacks, in a hearing of the US House of Representatives Committee on Homeland Security concerning the controversial use of facial recognition and other biometric technologies to capture data about travelers at US borders, US Customs and Border Protection continued to point prominently to The 9/11 Commission Report to justify the agency's use of facial recognition technology at US ports of entry.[9] In a 2023 speech, then-Secretary of Homeland Security Alejandro Mayorkas described the 9/11 airplane hijackings in detail before highlighting information-sharing as a way the US was filling "the gaps in our defenses" that he said the hijackers had exploited.[10]

The increasing collection and storage of data about individuals was, indeed, part of the US government's response to the 2001 attacks: for example, then-president George W. Bush created a secret surveillance program to collect information from telephone calls and e-mails between the US and other countries, and the government created scores of "fusion centers" devoted to increasing information-sharing between federal, state, and local law enforcement authorities.[11] In 2002, the US Defense Department revealed that it had created a program called "Total Information Awareness" (TIA), through which it aimed to find people who might pose a threat by mining large amounts of data from private and government sources—without a warrant.[12]

---

8 For an academic assessment also tracing the increasing US emphasis on data-gathering and mining for law enforcement purposes to the 9/11 attacks and perceptions of their causes, see Daniel J. Steinbock, "Data Matching, Data Mining, and Due Process," *Georgia Law Review*, vol. 40 (2005), p. 5.

9 House Committee on Homeland Security, "About Face: Examining the Department of Homeland Security's Use of Facial Recognition and Other Biometric Technologies," testimony of John Wagner, July 10, 2019, video available at https://www.congress.gov/event/116th-congress/house-event/109753, (accessed September 17, 2025), beginning at 16:23.

10 Department for Homeland Security, "Secretary Mayorkas Remarks at the 2023 International Counterterrorism Conference," May 31, 2023, available at https://www.dhs.gov/news/2023/05/31/secretary-mayorkas-remarks-2023-international-counterterrorism-conference (accessed September 17, 2025).

11 James Risen and Eric Lichtblau, "Bush Lets U.S. Spy on Callers Without Courts," *New York Times,* December 16, 2005, https://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html (accessed September 17, 2025); US Senate Permanent Subcommittee on Investigations, *Federal Support for and Involvement in State and Local Fusion Centers,* October 3, 2012, p. 1, https://www.hsgac.senate.gov/imo/media/doc/10-3-2012%20PSI%20STAFF%20REPORT%20re%20FUSION%20CENTERS.2.pdf (accessed September 17, 2025).

12 John Markoff, "THREATS AND RESPONSES: INTELLIGENCE; Pentagon Plans a Computer System That Would Peek at Personal Data of Americans," *New York Times*, November 9, 2002, https://www.nytimes.com/2002/11/09/us/threats-responses-intelligence-pentagon-plans-computer-system-that-would-peek.html (accessed September 17, 2025).

At the same time, a data mining entrepreneur named Hank Asher (now deceased) – who had pioneered the creation of major private databases of personal information – invented a new program called the Multi-state Anti-Terrorism Information Exchange (MATRIX) to assist the FBI with its hunt for the 9/11 attackers' associates.[13] In 2003, the newly established Department of Homeland Security provided a grant to support states' access to the database.[14]

These developments were extremely controversial at the time: civil liberties groups as well as state officials and elected representatives from both major parties objected to massive data-mining programs for law enforcement such as TIA and MATRIX. For example, the American Civil Liberties Union decried TIA as possibly "the closest thing to a true 'Big Brother' program that has ever been seriously contemplated in the United States," while officials in Georgia expressed concerns about the legal complexities and "potential for abuse" in sharing driver's license data from the state.[15] Federal and state agencies eventually shut down or stopped supporting TIA and MATRIX.[16]

The 9/11 Commission itself took a nuanced view of information-sharing in its 2004 report, concluding that although assessments of whether the attacks could have been prevented often described "problems of [a lack of] 'watchlisting,' of 'information sharing,' or of 'connecting the dots,'" such issues constituted "the symptom, not the disease."[17] In the Commission's view, the underlying problem was one of bureaucratic structure and culture: for example, a lack of clarity concerning which agency was responsible for a particular investigation, or a failure of agencies to coordinate or take joint action.[18] The Commission also observed that while the "storehouse" of information available to agencies was "immense," the government had "a weak system for processing and using what it ha[d]."[19] The Commission viewed information-sharing as part of the solution, but was considering only one specific context – transnational violence.[20] The Commission was also concerned about accountability, suggesting that queries of intelligence systems should leave an "audit trail."[21]

Yet, with nothing in US law to stop their creation, large collections of personal data for law enforcement use have proliferated in the years since the TIA and MATRIX controversies—to the extent that the practice of warrantless access to such data has become normalized, as the cases in this report illustrate. As police access to such vast databases has become ever more

---

13 Michael Schnayerson, "The Net's Master Data-Miner," *Vanity Fair,* Dec. 2004, http://www.vanityfair.com/news/2004/12/matrix200412 (accessed September 17, 2025).

14 Ibid.

15 American Civil Liberties Union, "Q&A on the Pentagon's 'Total Information Awareness' Program," April 20, 2003, https://www.aclu.org/documents/qa-pentagons-total-information-awareness-program (accessed September 17, 2025); Letter from Marshall Horne, Georgia Department of Motor Vehicle Safety, to Jim Lientz, September 29, 2003, available at (accessed May 9, 2024). https://www.aclu.org/documents/georgia-dmv-security-concerns-matrix (accessed September 17, 2025).

16 See, e.g., American Civil Liberties Union, "ACLU Applauds End Of 'MATRIX' Program," April 15, 2005, https://www.aclu.org/press-releases/aclu-applauds-end-matrix-program (accessed September 17, 2025).

17 National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report*, 2004, p. 400, https://www.9-11commission.gov/report/911Report.pdf (accessed September 17, 2025).

18 Ibid.

19 Ibid., pp. 416-417.

20 Ibid., pp. 416-418.

21 Ibid., p. 418.

commonplace, public objections by US civil liberties groups appear to have become rarer (with the exceptions of activism against certain specific collections of data, such as "gang" databases and pools of DNA, facial recognition or other biometric information).

However, in our view, large databases of personal information compiled for or marketed to police pose the same threats to rights that they did in the years shortly after the 9/11 attacks—and the need to understand and address them remains just as urgent. There is also a risk that such database use is seeping into deadly military operations, as in 2024 when Israel reportedly applied artificial intelligence to a large database to identify tens of thousands of people as targets "based on their apparent links to Hamas."[22]

b. The private sector: "Big data" as a commodity

As what became popularly known as a "collect it all" approach[23] gained currency within the US government, a different concept drove the gathering of increasingly vast quantities of personal data by private-sector companies: the idea of personal information as a marketable commodity. Today, evidence suggests that US police are a significant customer base for this for-profit market, which remains legal.

In 1992, data mining entrepreneur Hank Asher established a company called Database Technologies (DBT) to sell a datamining program he had developed to enable police and private insurers to conduct searches of Florida Department of Motor Vehicles data.[24] Hundreds of law enforcement bodies, including the FBI and DEA, signed contracts with DBT, and Asher's skills later led to the development of the large database Accurint, which included public and other records and is now part of LexisNexis, owned by RELX Group.[25] (Accurint is discussed in greater detail below.) Other data companies created similarly large digital collections of personal information such as ChoicePoint, which RELX Group also owned at the time of writing.[26] To the best of our knowledge, these databases and police access to them were (and are) legal under US law.

As early as 2004, academics and other experts were warning that the information in these massive databases was available to law enforcement and could lead to a fundamental shift in policing techniques. Privacy scholar Chris Hoofnagle – while taking a nuanced view of police access to large collections of personal data – warned that this access could result in abuses if not

---

22 Bethan McKernan and Harry Davies, "'The machine did it coldly': Israel used AI to identify 37,000 Hamas targets," *Guardian*, April 3, 2024, https://www.theguardian.com/world/2024/apr/03/israel-gaza-ai-database-hamas-airstrikes (accessed September 17, 2025).

23 See, e.g., Glenn Greenwald, "The crux of the NSA story in one phrase: 'collect it all,'" *Guardian*, July 15, 2013, https://theintercept.com/2015/05/28/nsa-officials-privately-criticize-collect-it-all-surveillance/ (accessed September 17, 2025).

24 Schnayerson, "The Net's Master Data-Miner"; Ann Woolner, "Ex-Drug Smuggler Turned Data Miner Reclaims Field He Created," *Bloomberg*, Sept. 15, 2011, http://www.bloomberg.com/news/articles/2011-09-15/ex-cocaine-smuggler-turned-data-miner-seeks-to-conquer-a-field-he-created (accessed September 17, 2025).

25 Schnayerson, "The Net's Master Data-Miner"; "FBI, DEA suspend online contracts," Associated Press, July 4, 1999 (on file with authors); RELX, "Acquisition of Seisint," July 14, 2004, https://www.relx.com/media/press-releases/archive/14-07-2004 (accessed September 17, 2025); LexisNexis, "About LexisNexis," https://www.lexisnexis.com/en-us/about-us/about-us.page (describing LexisNexis as "a division of RELX) (accessed September 17, 2025).

26 Electronic Privacy Information Center, "Choicepoint," undated, https://epic.org/privacy/choicepoint/ (accessed September 17, 2025); RELX, Press release, "Acquisition of Choicepoint Inc. Completed," September 19, 2008, https://www.relx.com/media/press-releases/archive/19-09-2008 (accessed September 17, 2025).

subject to rights-protecting restrictions. "The information could be used for political or personal purposes," he wrote, adding, "There is also a general risk that the collection of information on individuals will upset the balance between government and individuals, resulting in a shift of power that is oppressive."[27]

Our research suggests that this warning about oppressive police uses of this data was prescient—even if those uses are permitted under current US federal or state law, as they typically are.

The evolution of computing power and people's adoption of electronic devices, such as smartphones, to carry out everyday tasks and share extensive personal information online has greatly increased the amount of data that private companies known as "data brokers" can gather, store, and mine. The US legislature has long been aware of this phenomenon: in a 2013 report, the US Senate Committee on Commerce, Science, and Transportation observed,

> *[Consumers] use the Internet and their smart phones and tablets to make purchases, research medical conditions, plan vacations, interact with friends and relatives, do their jobs, map travel routes, and otherwise pursue their interests. With these activities, consumers are creating a voluminous and unprecedented trail of data regarding who they are, where they live, and what they own.*[28]

The result, the committee wrote at the time, was a "multi-billion dollar industry that largely operates hidden from consumer view" and allows information that once required the effort of a trip to the archives to be accessed with the touch of a button.[29]

---

27 Chris Jay Hoofnagle, "Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement, *North Carolina Journal of Law and Commercial Regulation*, vol. 29 (2004), pp. 595-597.

28 US Senate Committee on Commerce, Science, and Transportation, *A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes*, December 18, 2013, p. i.

29 Ibid.

However, the committee's analysis – like other government reports on the topic[30] – did not delve into how US police participate in this market in ever more detailed personal information, and the issue has received little government scrutiny in the years since. Yet, the reasons for concern about data sellers' practices have not ceased, as evidenced by the launch of a public inquiry by the federal Consumer Financial Protection Bureau in 2023.[31]

c. The data-broker industry

Today, the digitized personal data that police forces use when looking someone up – including when they are investigating suspected crimes or traffic offenses, but also when they are merely curious – may come from private sector databases, built by what media sources and civil liberties groups often describe as "data brokers." The term refers to a heterogeneous range of private companies that collect, categorize, analyze and sell personal data and profiles for profit – all activities that the law permits, except where specific prohibitions (discussed below) apply. Data brokers can lawfully obtain people's data from a variety of sources, which may include public records, commercial sources, web scraping, and online tracking on websites or apps that agree to sell the data to the data broker (often in exchange for marketing insights into their users), among others.[32]

For the avoidance of doubt, we emphasize that US laws in this area are permissive and that to the best of our knowledge, the companies mentioned in this report are operating and have operated within the law. We are also not suggesting that the companies intend to facilitate lookups based on mere curiosity or other actions that we would describe as misuse; to the contrary, it is common for US technology and data companies to require users to agree in writing not to misuse the systems. Our focus here is on the lack of legal safeguards – such as a warrant requirement imposed by law – and official accountability.

Online tracking is a key source of data for data brokers. The hundreds or thousands of interactions nearly everyone in the US has with digital services nowadays are recorded and stored in various companies' databases. The companies may then aggregate these troves of data, combine them with other information they have bought or collected, and analyze them to create profiles of (and, sometimes, predictions about) people, which they then sell to myriad companies that benefit from knowing their users or customers intimately—usually because they want to market products and services more efficiently.[33]

---

30 US Government Accountability Office, *Information Resellers: Consumer Privacy Framework Needs to Reflect Changes in Technology and the Marketplace,* September 2013; Federal Trade Commission, *Data Brokers: A Call for Transparency and Accountability,* May 2014.

31 Consumer Financial Protection Bureau, Press release, "CFPB Launches Inquiry Into the Business Practices of Data Brokers," March 15, 2023, https://www.consumerfinance.gov/about-us/newsroom/cfpb-launches-inquiry-into-the-business-practices-of-data-brokers/ (accessed September 17, 2025).

32 Privacy International, "How do data companies get our data?", May 25, 2018, https://privacyinternational.org/long-read/2048/how-do-data-companies-get-our-data (accessed September 17, 2025).

33 Privacy International, "I asked an online tracking company for all of my data and here's what I found", November 7, 2018, https://privacyinternational.org/long-read/2433/i-asked-online-tracking-company-all-my-data-and-heres-what-i-found (accessed September 17, 2025).

However, especially since 9/11, some data brokers have found a lucrative alternative revenue source: governments. Various government and law enforcement agencies have, for years, eyed data they did not have the technology (or, arguably, the legal power) to gather directly by themselves, but that private companies can and often do legally gather. Some of these purchases have been relatively widely reported and controversial: for example, the FBI has bought location data,[34] and US customs and border authorities have bought smartphone location data.[35] Many other sales of data from data brokers to US police remain overlooked or – increasingly – routinized. As discussed below, government entities also produce data on which some data brokers rely, in the form of public records. Again, we are not alleging that private companies' sales or donations of people's personal data to the government have been illegal or that companies are knowingly helping police evade requirements for warrants or court orders. In many circumstances, there are no such requirements in US law—and that, we say, is the problem.

ii. A tattered patchwork: US data privacy laws

Although the US Congress has long been on notice that the government and the private sector in the country have the ability and strong incentives to collect large amounts of personal data, it has placed few legal limitations on these activities over the years. More than a decade after the Senate Commerce Committee report quoted above, there have been no major relevant reforms in federal privacy law.

The laws that do exist often focus on the source of the information or the technical means of obtaining it rather than what the data consists of or what it could reveal; this approach means that if government or private entities cannot legally gather data from one source, they are often legally free to obtain the same information from another one. We are not suggesting that companies or government-run databases deliberately enable an evasion of the law, but rather that the US legal environment around personal data is permissive and that legally mandated restrictions are the exception rather than the rule.

34 Wired, "The FBI Just Admitted It Bought US Location Data", March 8, 2023, https://www.wired.com/story/fbi-purchase-location-data-wray-senate/ (accessed September 17, 2025).

35 404 Media, "Customs and Border Protection Says It Will Stop Buying Smartphone Location Data", September 12, 2023, https://www.404media.co/customs-and-border-protection-stop-buying-location-data/ (accessed September 17, 2025).

Under federal law and regulations, as well as US Supreme Court case law, some protections currently exist for:

- **Communications content and records.** Under the Electronic Privacy Communications Act (adopted in 1986), communications service providers such as telephone and internet companies cannot disclose the content of stored communications to anyone else without the subscriber's consent, except in limited circumstances such as when police have obtained an appropriate court order.[36] Records of communications, such as a list of the numbers a telephone subscriber has dialed, are only available to police through legal process such as a subpoena (a formal order a government agency can issue without a judge's approval).[37] Police need a warrant from a court – or, a recognized exception to the usual warrant requirement must apply – before intercepting the content of private communications in real time.[38] However, as discussed elsewhere in this report, private data brokers can and do lawfully obtain data linking individuals to telephone numbers – which police can then retrieve from these databases, even though they would need a subpoena to obtain the same information from the telephone company.

- **Location data—if historical and held by a communications service provider.** In its 2018 decision in Carpenter v. United States, the US Supreme Court ruled that police need a warrant to obtain historical data about the location of someone's cell phone from a communications service provider. The court did not address whether police need a warrant to obtain such data in real time or from another source, explicitly leaving these issues open.[39]

- **Driver's license records—subject to exceptions.** In the US, driver's licenses are issued by states and territories and are an extremely common form of identification. To obtain a license, an individual typically must sit for a photograph and provide demographic and biometric information such as home address, date of birth, hair color, eye color, height, and weight. The federal Driver's Privacy Protection Act (DPPA) generally prohibits the authorities that issue such licenses from disclosing the personal information they collect in this manner, but this restriction is subject to exceptions that can allow businesses to obtain at least some of the data.[40] The DPPA also contains a broad exception allowing the disclosure of driver's license data "[f]or use by any government agency, including any … law enforcement agency, in carrying out its functions."[41] As noted elsewhere in this report, police access to driver's license data from government-run databases has resulted in abuses and controversy.

---

36 18 U.S.C. §§ 2702-2703.

37 18 U.S.C. § 2703(c)(2).

38 *Katz v. United States*, 389 U.S. 347 (1967). Court decisions referenced in these footnotes without mention of a specific jurisdiction are US Supreme Court decisions and are freely available online.

39 *Carpenter v. United States*, 585 U.S. 296 (2018).

40 18 U.S.C. § 2721.

41 18 U.S.C. § 2721(b)(1).

- **Some health information and records.** The US Department of Health and Human Services has adopted regulations barring health care providers and insurance companies from selling information about the health of identifiable people, and imposing other limits on the disclosure of such information.[42] However, data brokers can still gather data that may reveal information about people's health from other sources. Police can also obtain health information from insurance companies and care providers with a subpoena or court order, or in certain other limited circumstances.[43]

- **Some financial information.** Businesses that qualify as consumer reporting agencies (CRAs) under the Fair Credit Reporting Act (FCRA) may only disclose personal data that amounts to a "consumer report" in response to a court order, to an employer, or in certain other limited circumstances.[44] If a business is a CRA, then a wide range of personal information it holds may count as a "consumer report" and be subject to these disclosure restrictions; examples include information about creditworthiness, "character," and "mode of living," depending on how the data will be used.[45] However, the FCRA is complex, and data brokers often maintain that the information they offer to police and others is not subject to the act's restrictions.[46]

  Financial institutions such as banks and loan providers must comply with the Gramm-Leach-Bliley Act, which requires that income information, bank account and credit card numbers, and certain other financial information be kept confidential.[47]

- **Education records.** Educational institutions that receive federal funding cannot disclose students' records except in specific, limited circumstances, and disclosures to police require legal process.[48]

---

42 45 C.F.R. § 164.502(a)(5)(ii).

43 US Department of Health and Human Services, "Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule: A Guide for Law Enforcement," undated, https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/special/emergency/final_hipaa_guide_law_enforcement.pdf (accessed September 17, 2025).

44 15 U.S.C. §§ 1681a-b.

45 15 U.S.C. §§ 1681a.

46 See, e.g., TransUnion, "TLO Subscriber Agreement Additional Terms and Conditions," September 12, 2025, https://www.transunion.com/legal/terms-of-use/tlo (accessed September 17, 2025) ("The TLOxp solution is not provided by a consumer reporting agency and does not constitute a consumer report as these terms are defined by the Fair Credit Reporting Act"); Thomson Reuters, "Thomson Reuters CLEAR," https://legal.thomsonreuters.com/en/products/clear-investigation-software (accessed May 9, 2024) ("Thomson Reuters is not a consumer reporting agency and none of its services or the data contained therein constitute a 'consumer report' as such term is defined in the Federal Fair Credit Reporting Act"); LexisNexis, "Accurint," https://www.accurint.com/ (accessed May 9, 2024) ("The Accurint services are not provided by 'consumer reporting agencies,' as that term is defined in the Fair Credit Reporting Act ... and do not constitute 'consumer reports,' as that term is defined in the FCRA").September 17, 2025) ("Thomson Reuters is not a consumer reporting agency and none of its services or the data contained therein constitute a 'consumer report' as such term is defined in the Federal Fair Credit Reporting Act"); LexisNexis, "Accurint," https://www.accurint.com/ (accessed September 17, 2025) ("The Accurint services are not provided by 'consumer reporting agencies,' as that term is defined in the Fair Credit Reporting Act ... and do not constitute 'consumer reports,' as that term is defined in the FCRA").

47 Federal Trade Commission, "FTC Safeguards Rule: What Your Business Needs to Know," December 2024, https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know (accessed February 5, 2026).

48 20 U.S.C. § 1232g(b).

- **Information that website operators collect from children under 13 years of age.** Companies that operate online sites or services must comply with regulations adopted by the Federal Trade Commission (FTC) that bar them from collecting, using, or disclosing information from children under 13 without parental consent.[49] The effectiveness of these regulations, especially in an era of social media apps that may hold appeal for children, has been a subject of much debate.[50]

- **Financial, educational, criminal, medical, and other records the federal government holds about people—subject to exceptions.** The Privacy Act of 1974 states that government agencies that hold information about US citizens or lawful permanent residents (green-card holders) can only disclose that information in response to a court order or in certain other specified circumstances. However, the act permits disclosures for law enforcement purposes and allows agencies to exempt arrest, charging, and other criminal records from protection.[51]

An executive order that then-president Donald Trump issued shortly after taking office for the first time in 2017 directed federal agencies to exclude people who were not US citizens or green-card holders from Privacy Act protections.[52] Then-president Joe Biden revoked this order in 2021, but similar orders remain possible, and a March 2025 order by re-elected President Trump may have had an effect akin to the 2017 order.[53]

Additionally, under the Federal Trade Commission Act (FTCA), companies cannot engage in "unfair or deceptive acts or practices."[54] A suspected breach of this restriction can result in an investigation by the FTC and an order to halt such behaviors; the violation of such an order can result in a fine.[55] These provisions of the act do not apply to law enforcement agencies—and even where corporate practices are concerned, the FTC faces practical constraints such as resource limitations in investigating potentially unfair or deceptive treatments of data.[56]

---

49 15 U.S.C. § 6502(a); 16 C.F.R. § 312.3.

50 See, e.g., Natasha Singer, "At Meta, Millions of Underage Users Were an 'Open Secret,' States Say," *New York Times,* November 25, 2023, https://www.nytimes.com/2023/11/25/technology/instagram-meta-children-privacy.html (accessed September 17, 2025).

51 5 U.S.C. § 552a(b)(7), (j)(2).

52 "Executive Order: Enhancing Public Safety in the Interior of the United States," January 25, 2017, § 14, archived at https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-enhancing-public-safety-interior-united-states/.

53 "Executive Order on the Revision of Civil Immigration Enforcement Policies and Priorities," January 20, 2021, https://www.federalregister.gov/documents/2021/01/25/2021-01768/revision-of-civil-immigration-enforcement-policies-and-priorities; Executive Order, "Stopping Waste, Fraud, and Abuse by Eliminating Information Silos," https://www.whitehouse.gov/presidential-actions/2025/03/stopping-waste-fraud-and-abuse-by-eliminating-information-silos/; see also Electronic Privacy Information Center, Press release, "Latest Executive Order Threatens to Shred Federal Privacy Protections, Hoard Personal Data for DOGE Use," March 21, 2025, https://epic.org/press-release-latest-executive-order-threatens-to-shred-federal-privacy-protections-hoard-personal-data-for-doge-use/ (accessed February 5, 2026).

54 15 U.S.C. § 45(a)(1).

55 15 U.S.C. § 45(b), (l).

56 Chris Jay Hoofnagle et al., "The FTC can rise to the privacy challenge, but not without help from Congress," Brookings, August 8, 2019, https://www.brookings.edu/blog/techtank/2019/08/08/the-ftc-can-rise-to-the-privacy-challenge-but-not-without-help-from-congress/ (accessed September 17, 2025).

Under the Computer Fraud and Abuse Act (CFAA), it is a crime for police – or anyone else – to obtain government-held data by "intentionally access[ing] a computer without authorization or exceed[ing] authorized access."[57]As noted below, the law has sometimes been used to prosecute police who have allegedly used law enforcement databases to search for information without a policing purpose, including to look up information about women in whom they were romantically interested. However, it appears that very few of the cases described in this report have resulted in prosecutions of officers under the CFAA or other federal or state criminal laws.

These porous protections leave vast amounts of information about people up for grabs by data brokers and others.

In the absence of stronger efforts by the federal government to protect personal data from exploitation and abuse, some states have taken at least limited actions. For example, in 2018, California and Vermont passed consumer privacy laws intended to increase transparency about the information data brokers hold and impose other checks.[58] Some states also have laws or other protections regarding specific types of personal data such as driver's license information.[59] Additionally, some police departments have policies making the misuse of stored personal data an infraction subject to discipline.[60]

iii. A global comparison: International, regional, and national data privacy standards

a. International human rights law

The International Covenant on Civil and Political Rights (ICCPR), which the US has signed and ratified, recognizes a human right to freedom from "arbitrary or unlawful" government interferences with privacy, as well as reputation.[61] Under this provision, police and other government agencies should not gather, store, or search personal data in a manner that interferes with privacy unless these activities are clearly authorized by law and subject to safeguards

57 18 U.S.C. § 1030(a)(2).

58 Californians for Consumer Privacy, "About the California Consumer Privacy Act," https://www.caprivacy.org/about (accessed September 17, 2025); Adam Schwartz, "Vermont's New Data Privacy Law," Electronic Frontier Foundation, September 27, 2018, https://www.eff.org/deeplinks/2018/09/vermonts-new-data-privacy-law (accessed September 17, 2025);

59 See, e.g., National Immigration Law Center, "Protecting State Driver's License Information," updated August 2025, https://www.nilc.org/resources/protecting-state-drivers-license-information/ (accessed September 17, 2025).

60 See, e.g., Phoenix Police Department, "Policy Violations Index," Operations Order 2.1.01, 18 February 2025, https://public.powerdms.com/PhoenixPD/documents/1598916 (accessed September 17, 2025),Order 4B(1)(d) ("Obtaining any information for personal use via the record management system/s, such as MDC/CAD/National Crime Information Center (NCIC)/Arizona Crime Information Center (ACIC)" is a "Class I violation," which can lead to "an eight (8) or 24-hour suspension without pay.") and Order 4C(1)(d) (" Disseminating information obtained from the record management system/s, such as MDC/CAD/NCIC/ACIC, or other public safety databases, without authorization or not within guidelines of the Terminal Operator Certification (TOC) process" is a "Class II violation," which can lead to "a 24 or 40 hour suspension without pay and possible demotion.")

61 ICCPR, Article 17.

that are strong enough to prevent abuses.[62] Officials should also refrain from engaging in such activities unless they are necessary for achieving a legitimate aim and are the least intrusive method available.[63]

However, the US Congress has never incorporated the ICCPR into domestic law, meaning that individuals are unable to rely on their rights under the Covenant in US courts. Additionally, we note for clarity that the ICCPR formally only constrains government actors (such as police), not private companies.

Nevertheless, the United Nations Human Rights Committee has stated that to respect the human right to privacy, governments should regulate how companies collect, store, and share personal data; they should also take steps to prevent the misuse of such information to violate other rights.[64] The UN Office of the High Commissioner on Human Rights has described a "growing global consensus" on data protection—specifically, "minimum standards that should govern the processing of personal data by States, business enterprises and other private actors."[65] These minimum standards include the principles that "[p]ersonal data processing should be necessary and proportionate to a legitimate purpose that should be specified by the processing entity" and that "[c]hanges of purpose without the consent of the person concerned should be avoided and when undertaken, should be limited to purposes compatible with the initially specified purpose."[66] The sharing of private-sector data with law enforcement would appear to constitute a change in purpose to which most individuals have not knowingly consented, and to differ sharply from the original purpose; there also does not appear to be any other kind of blanket legal authorization for it.

Additionally, UN experts and human rights courts increasingly conclude that individuals can have privacy interests even in information that is publicly available – for example, data about someone's movements through public places or information they have posted on a social media site. The UN Human Rights Committee emphasized in 2020, regarding the freedom of assembly, that the international human right to privacy may still apply if people expose their faces in public (rendering them vulnerable to facial recognition technology) or describe protest plans or actions on social media.[67]

---

62 UN OHCHR, "The right to privacy in the digital age," A/HRC/27/37, June 30, 2014, ¶ 28.

63 UN OHCHR, "The right to privacy in the digital age," A/HRC/29/39, August 3, 2018, ¶ 10.

64 UN Human Rights Committee, "General Comment no. 16: Article 17 (Right to privacy)," U.N. Doc. HRI/GEN/1/Rev. 1, April 8, 1988, ¶ 10.

65 UN OHCHR, "The right to privacy in the digital age," A/HRC/39/29, August 3, 2018, ¶ 29.

66 Ibid.

67 United Nations Human Rights Committee, General Comment no. 37 (2020) on the right of peaceful assembly (article 21), UN Doc. CCPR/GC/37 (September 17, 2020), para. 62 ("The mere fact that a particular assembly takes place in public does not mean that participants' privacy cannot be violated. The right to privacy may be infringed, for example, by facial recognition and other technologies that can identify individual participants in a crowd. The same applies to the monitoring of social media to glean information about participation in peaceful assemblies").

b. European Union standards – the GDPR and the Law Enforcement Directive

In 2016, the European Union adopted one of the most comprehensive and exacting sets of data protection laws in the world. The General Data Protection Regulation ("GDPR")[68] governs data processing by private entities and public bodies, while the Law Enforcement Directive ("LED")[69] governs data processing for law enforcement purposes (i.e., by police and criminal justice agencies).

These EU laws establish data protection principles, such as transparency, purpose limitation, and data minimization; provide rights to data subjects; and impose obligations on data processors. They apply to the processing of "personal data," defined as "any information relating to an identified or identifiable natural person."[70]

The LED, which all EU Member States must adopt into national legislation in some form, mandates in particular that:

- Personal data must be "collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes."[71]

- Processing will be lawful "only if and to the extent that processing is necessary for the performance of a task carried out by a competent authority for the purposes set out in Article 1(1)" ("the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security").[72]

- The processing of sensitive personal data ("personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation") must be allowed only where strictly necessary, subject to appropriate safeguards and only where authorized by law, to protect the vital interests of the data subject or of another person, or where the data was manifestly made public by the data subject.[73]

---

68 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

69 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

70 GDPR, n 66, Article 4(1).

71 LED, n 67, Article 4(1)(b).

72 LED, n 67, Article 8(1).

73 Ibid, Article 10.

Under this framework, police in the EU are only permitted to acquire personal data if they can demonstrate that doing so is necessary for the performance of their criminal justice tasks—which includes demonstrating that no less intrusive means can achieve the same purpose, and that only personal data which is adequate and relevant for the purposes of the processing is collected and processed.[74] This is a high standard, and one that – in our view – would not allow the blanket acquisition of, or unfettered access to, data. Only when the data is necessary to an investigation, likely about people who are live suspects, victims of or witnesses to an alleged criminal offence, should it be collected. Even data about people who have previously been convicted of an offence would be subject to protections.[75]

If police forces in the EU acquired data from private entities instead of through their own investigative techniques, the GDPR, and the rules it imposes on data processing by private entities, would be relevant. Even if the police could demonstrate the lawfulness of processing the data under the LED, if this data was initially collected by private entities in breach of the GDPR, then any subsequent sharing or use would be unlawful.

However, collection and processing by data brokers is often opaque, difficult to trace, and difficult to challenge. Data brokers often amass data from third-party sources that themselves may not have complied with the GDPR when collecting data from or about individuals (including because, in many instances, those third-party sources are likely not subject to the GDPR). Many of these sources may rely on lawful bases such as consent, but could be unable to demonstrate that the consent was of the nature and quality required by the GDPR.[76] (We are not alleging here that any private entity has breached the GDPR in this manner.)

Therefore, under these EU legal standards, it is highly unlikely that police forces in the EU would be able to lawfully acquire or gain access to data from private entities on a massive scale, even if that data was originally lawfully collected and processed by a third party.

c. UK expansion of data access powers

The UK government has recently adopted changes to the Investigatory Powers Act 2016, which regulates the conduct of the UK intelligence services where surveillance is concerned. The Investigatory Powers (Amendment) Act 2024 authorises intelligence services to access "third party bulk personal datasets," "whether on payment or otherwise" (subject to a warrant granted by the Secretary of State for the Home Department, who is part of the executive branch).[77] In our view, this change opens the door to intelligence agencies such as MI5, MI6, and GCHQ purchasing datasets from data brokers and any other private entities. Although this power would not yet extend to police forces, the police could in some instances request access from the intelligence services to data contained in a third-party bulk personal dataset, if related to an investigation.[78]

---

74 European Data Protection Supervisor (EDPS), "Necessity & Proportionality," https://edps.europa.eu/data-protection/our-work/subjects/necessity-proportionality_en (accessed September 17, 2025).

75 LED, n 67, Article 6.

76 GDPR, Article 7.

77 Investigatory Powers (Amendment) Act 2024, Part 1, section 5.

78 See also discussion below about current access to Experian's 'Investigator Online' service by UK police forces.

B.
This is your life: What the databases include

Instant access to large collections of data about people is an integral part of US policing today, to such a great extent that one scholar has described these systems and their easy availability as having "fostered a revolution in policing akin to that of the introduction of patrol cars and two-way radios."[79] Yet, most people in the United States, including lawmakers, likely are not aware of the full scope of this information – and how much it can reveal about personal life, race and other physical characteristics, relationships, and past interactions with police.

79 Wayne A. Logan, "Policing Police Access to Criminal Justice Data," 104 IOWA L. REV. 620 (January 2019), p. 621.

i. Massive law enforcement databases

Our research indicates that the US private sector has developed large collections of personal data with law enforcement in mind, and several of these are described below. However, the government, too, has created enormous and easily accessible databases intended for police use.

a. The National Crime Information Center (NCIC)

One government data collection that features in many of the civil liberties lawsuits and other relevant cases we examined is the NCIC database, which contains data from both federal and state sources. The FBI operates this database and makes its contents available to state, local, and tribal police throughout the country and (it has previously said) in Canada.[80]

Today, this system receives heavy use: the FBI website states that the database holds "more than 18 million active records and averages millions of transactions each day."[81]

While the FBI hosts the database, it is the state and federal agencies that have access to it that are responsible for entering, altering or deleting records, the website explains.[82] Where criminal histories are concerned, federal regulations place the onus for accuracy and completeness on the agency contributing the data.[83]

A federal agent testifying in a federal criminal trial in Albuquerque, New Mexico following the "Surge" operation discussed in section IV(c)(ii) below stated candidly that "NCIC is only as good as what people put into it. You'll find some jurisdictions, they simply don't mail in or send the information to NCIC so it can be an accurate reflection."[84]

An undated NCIC operating manual posted online by the state of Massachusetts indicates that the FBI periodically conducts "compliance audit[s]" of other agencies to check for the accuracy and security of data entered into the system, among other matters.[85] Federal regulations also provide that agencies that neglect to ensure the accuracy and completeness of criminal history data they contribute may lose their access to the system.[86] However, there appears to be no

---

80 Federal Bureau of Investigation, "National Crime Information Center (NCIC)," https://www.fbi.gov/services/cjis/ncic, version accessed on August 21, 2019. (As at September 17, 2025, this page no longer mentions Canada.)

81 As at 2023. See Federal Bureau of Investigation, "National Crime Information Center (NCIC)," https://www.fbi.gov/services/cjis/ncic (accessed September 17, 2025).

82 Ibid.

83 28 C.F.R. § 20.37. The inclusion of "III System" within NCIC is confirmed by 28 C.F.R. § 20.3.

84 *United States v. Jackson*, case no. 1:16-cr-2362 (D. N.M.), Transcript of Proceedings, Vol. I (doc. 62), November 18, 2017, p. 109.

85 *NCIC 2000 Operating Manual,* https://www.mass.gov/files/documents/2019/01/16/NCIC%202000%20Operating%20Manual_0.pdf, pp. 79-80 of PDF (accessed September 17, 2025). We note that "NCIC 2000" is what the manual calls the software; judging by the document's references to agencies such as DHS that were created after 9/11, we infer that the manual itself was published more recently than 2000, although it does not bear a date.

86 28 C.F.R. 20.37-38.

federal legal obligation on the FBI or other agencies to update, correct, or delete data, even though the NCIC website refers to "measures to ensure the privacy and integrity of the data" such as validation of records by contributing agencies.[87]

The data stored about people in the NCIC system is extremely wide-ranging, with categories including "Gang," "Wanted Person," "Immigration Violator," "Violent Person," and "Identity Theft," among others.[88] The "Violent Person" classification could include anyone whom a member of law enforcement "reasonably believes … has seriously expressed his or her intent to commit an act of unlawful violence against" police or some other member of the "criminal justice community," with no conviction required.[89] This broad category raises questions about the potential for abuse: there appears to be nothing to prevent an officer from simply declaring – wrongly, and potentially for racist reasons – that an individual has said they intend to hurt the police, perhaps because the individual has repeated a protest slogan or song lyric expressing resistance to police violence.

Testimony by the federal agent in the Albuquerque trial further indicates that NCIC places a potentially large amount of personal information at an officer's fingertips:

> *NCIC reports will have all of a person's identifying information; their name; any aliases; any different forms of their name that they've used; different spellings; date of birth; Social Security number; height; weight; sometimes it has their employment; previous addresses; state ID numbers; Department of Corrections numbers; any arrests and convictions that are submitted by the different jurisdictions.*[90]

The FBI writes that the "most recognizable" use NCIC "is by officers during routine traffic stops." While the Bureau highlights that the system could indicate whether a vehicle has been stolen, and cautions officers that "a positive response … from the NCIC doesn't establish probable cause for an officer to make an arrest," this recognized frequent use of a powerful database during traffic stops prompts questions about how often NCIC has been a factor in some of the abuses described in Section IV below.[91]

---

87 Federal Bureau of Investigation, "National Crime Information Center (NCIC)," https://www.fbi.gov/services/cjis/ncic (accessed 10 October 2025).

88 Ibid.

89 Federal Bureau of Investigation, "Crime Data: NCIC Violent Person File," November 7, 2023, https://leb.fbi.gov/bulletin-highlights/additional-highlights/crime-data-the-ncic-violent-person-file (September 17, 2025).

90 *United States v. Jackson*, Transcript of Proceedings, Vol. I (doc. 62), November 18, 2017, p. 109.

91 Federal Bureau of Investigation, "National Crime Information Center (NCIC)," https://www.fbi.gov/services/cjis/ncic (accessed September 17, 2025).

b. State databases

In addition to contributing data to the NCIC, many states have their own large repositories of personal data for easy law enforcement use. One system known as "Nlets" (or NLETS) describes itself as a non-profit organization created by agencies in all 50 US states, and lists the datasets available via its system as including (among others) driver's license and "Driver History" data, information related to gun licenses, "Criminal History," immigration status information through a database run by Immigration and Customs Enforcement, and information from automated license plate readers.[92] As of 2019, the organization's website said the system could enable access to "complete biographic and biometric data" about an individual.[93] The system also offers access to information from a range of Canadian databases.[94]

One example of a state-specific system, Pennsylvania's Commonwealth Law Enforcement Assistance Network (CLEAN) and Commonwealth Justice Network (JNET), together provide various state-level policing and drivers' records as well as a portal to Nlets and the NCIC.[95] The state has posted the forms for designating individuals in CLEAN and the NCIC as "Violent Person[s]," identity theft victims, or members of several other database categories; the "Violent Person" and identity theft forms invite officers to describe biometric and other potentially sensitive information such as the person's race, skin tone, ethnicity, scars, marks, and tattoos, and (for the "Violent Person" form) to indicate whether the person's DNA information is on file.[96]

In Michigan, police can gain access to personal data in the Law Enforcement Information Network (LEIN). Law enforcement agencies in the state can also "purchase license plate screening technology from vendors that provide devices and software capable of scanning license plates and comparing the data against key databases for records associated with those plates," including the NCIC's "Immigration Violator," "Gang," and "Wanted Person" databases, according to a state website.[97]

Ohio's Law Enforcement Automated Data System (LEADS) similarly "provides a repository of data available statewide and interfaces to the NCIC and NLETS systems," and offers access to searchable personal data including "driving records, vehicle ownership, stolen property, missing

92 Nlets, "Message Keys," https://www.nlets.org/resources/maps/message-keys/key (accessed September 17, 2025).

93 Nlets, "Mission & Vision," https://www.nlets.org/about/who-we-are (accessed May 9, 2024); Nlets, "Transactions," https://www.nlets.org/about/what-we-do (accessed August 29, 2019; see archived page at https://web.archive.org/web/20191103055756/https://www.nlets.org/about/what-we-do) .

94 Nlets, "Message Keys," https://www.nlets.org/resources/maps/message-keys/key (accessed September 17, 2025).

95 Pennsylvania State Police, "CLEAN," https://www.psp.pa.gov/law-enforcement-services/Pages/Commonwealth-Law-Enforcement-Assistance-Network.aspx (last accessed September 17, 2025).

96 Ibid., including "Violent Person CLEAN/NCIC Entry Worksheet" and "Identity Theft Victim CLEAN/NCIC Entry Worksheet" (available for download via links on the site).

97 Michigan State Police, "Access to the LEIN," https://www.michigan.gov/msp/0,4643,7-123-3493_72291-294058--,00.html (accessed September 17, 2025).

persons, warrants, and parole status," as well as driver's license photographs and "criminal histories."[98] The entity that maintains the interface for LEADS states that "[a]pproximately 17,000 devices throughout Ohio access the functions associated with" the system.[99]

These and other state databases may be subject to certain safeguards. For example, Ohio law seeks to ensure the accuracy of the data in the system, requiring that "[a]ll entries into the LEADS and NCIC files shall be reviewed and documented by a second person within the agency to verify the data entered matches the source document(s)" and that "[i]nvalid records or data must be removed from the files immediately."[100] Michigan criminalizes access to and use of "nonpublic information" in LEIN for personal reasons.[101] However, states generally do not appear to have adopted thorough checks on potential abuse to the extent recommended in this report.

As database and networking technology become cheaper and more ubiquitous, cities may also begin creating their own collections of personal data for law enforcement. For example, at the time of writing, officers in New York City had instant access via mobile phones and tablet computers to department databases as well as the Domain Awareness System, which the department has described as "one of the world's largest networks of cameras, license plate readers, and radiological censors."[102] (License plate reader data, which can be used to track a person's location and travel patterns, is discussed below.)

98 Northwest Ohio Regional Information System, "LEADS Interface," https://www.noris.org/multi-agency/leads-interface/ (accessed August 29, 2019; see https://web.archive.org/web/20190610194512/https://www.noris.org/multi-agency/leads-interface/).

99 Ibid.

100 Ohio Administrative Code § 4501:2-10-5.

101 Michigan Compiled Law 28.214(4)(3), (6).

102 New York City Police Department, "Technology," https://www1.nyc.gov/site/nypd/about/about-nypd/equipment-tech/technology.page (accessed September 17, 2025).

c. Police databases abroad – Mega-police database plans proposed in the UK

Police databases are a feature of many countries' infrastructures, with varying degrees of interoperability and safeguards. At the time of writing, UK police forces had access to two main databases: the Police National Computer (PNC), which holds mostly information relating to individuals arrested for or charged with crimes, and the Police National Database (PND), mostly a repository of intelligence data. For years, the Home Office had been trying to create the "Law Enforcement Data Service" (LEDS), a unified, common interface that would combine the PND and PNC and further data sources.[103]

However, sustained opposition by civil society, concerned particularly by the conflation of intelligence and evidence material, expansion of watchlists and potential use for immigration control,[104] had stalled the project. In November 2023, the Home Office "withdrew" the Data Protection Impact Assessment (DPIA) it had performed on LEDS in October 2020, indicating a potential change of course.[105]

As far as we know, there are no plans in the UK to integrate data sourced from private entities, such as data brokers, in any national police databases, nor to grant the police the right to access such data in bulk. However, the Investigatory Powers (Amendment) Act 2024 mentioned above provides legal powers for UK intelligence agencies to purchase datasets from data brokers and any other private entities. There is a possibility that police forces may exploit these new powers to request data from such datasets if they can argue they are collaborating with intelligence agencies or otherwise have the power to request specific data for their investigations.[106]

---

103 Privacy International, "UK Law Enforcement Data Service (LEDS): the new police mega-database", https://privacyinternational.org/campaigns/uk-law-enforcement-data-service-leds-new-police-mega-database (accessed September 17, 2025).

104 Privacy International, "Is over-policing the future?: Development of the UK Law Enforcement Data Service (LEDS)", August 13, 2020, https://privacyinternational.org/long-read/4122/over-policing-future-development-uk-law-enforcement-data-service-leds (accessed September 17, 2025).

105 Home Office, "Law Enforcement Data Service: Data Protection Impact Assessment," 24 December 2021, https://www.gov.uk/government/publications/law-enforcement-data-service-data-protection-impact-assessment (accessed September 17, 2025).

106 On police-intelligence service collaboration, see Data (Use and Access) Act 2025, s89.

C. Records by the billion: Data brokers sell personal information to police

i. Overview

Several major data brokers market databases specifically to US law enforcement, and their promotional materials have portrayed data collections that offer a thorough picture of millions of individuals' lives. For example, on a webpage marketing its TLOxp database to law enforcement, TransUnion – a credit reporting agency – stated prominently as of 2025 that the system contained "[d]ata on over 95% of the U.S. population," including "4 billion phone records," "4 billion address records," and "350 million Social Security numbers."[107] LexisNexis has claimed that Accurint users can search for links between people and phone numbers, as well as e-mail addresses.[108]

While some of the data that data brokers offer to US police is drawn from public records, other information comes from proprietary sources. Through some systems, officers can view every address and phone number associated (at least in the system) with a person's name, their Social Security number, the type and value of their car and home, and public information from their social media profiles. In a single place, they can see records purporting to show whether the person has ever been arrested (even if not convicted of any crime), filed for bankruptcy, been married or divorced, or been registered to vote. They can retrieve records based on partial names, fragments of license plate numbers, or car descriptions. They may be able to view photographs.

107 TransUnion, "TLOxp for Law Enforcement," https://www.tlo.com/law-enforcement (accessed September 17, 2025; also available in archived form at https://web.archive.org/web/20250709035723/https://www.tlo.com/law-enforcement). Here, "phone records" appears to mean information tying individuals to phone numbers, not records of calls or texts.

108 LexisNexis, "Accurint LE Plus: Accurint for Law Enforcement Plus User's Guide," pp. 9-10. As of 2019, this document was publicly available at https://aes.seisint.com/User_Guide.pdf and is now on file with the authors.

Though the full extent to which law enforcement agencies purchase this data is unclear, some public information about purchase and use is available. For example, federal procurement documents indicate that the Bureau of Alcohol, Tobacco, Firearms and Explosives (commonly known in the US as the "ATF") has purchased access to TLOxp since at least 2014 and likely still does, as its most recent purchase appears to have been in August 2025.[109]

Only a relatively small number of the cases discussed in this report concern police misuse of private, rather than government, databases. We also offer a reminder here that we are not claiming that the companies mentioned in this report are breaking the law or knowingly helping police behave unethically.

However, as is also the case for large government-run databases of personal information, police access to these private-sector databases does not legally require a warrant, other court order, or subpoena—all of which are forms of protection for individual rights or at least leave a record via official channels for accountability purposes. Instead, all police departments need to do is purchase access to the systems.

It is possible that relatively few federal civil rights lawsuits have described police misuses of private-sector databases because the police do not rely on these systems as often as they rely on government-run ones such as NCIC, and it is also possible that police use of private-sector systems results in fewer abuses or mistakes.

However, it also appears possible to us that police or prosecutors are not disclosing the use of for-profit databases to people who have been prosecuted or arrested, or who otherwise experience situations that prompt them to file civil rights lawsuits; this would mean that law- and policymakers do not have a full picture of how, and how often, police use the databases. Prior research by Human Rights Watch and US media outlets concerning the practice of "parallel construction" – law enforcement and intelligence agencies' deliberate creation of alternative explanations for how they found evidence or information – prompts concerns that police may be using these private databases without disclosing such activities to the people affected.[110] We also do not know whether or how police departments may be integrating personal data from private-sector collections into government-run databases or vice versa. We are not suggesting that such practices – if they are occurring – necessarily violate US law or that companies mean to facilitate them. What we wish to indicate here is that the US public, elected officials and courts may not have a complete understanding of whether and how police in their jurisdictions use personal data from privately run databases.

Many of the types of personal data that private companies offer to US police through large databases may be sensitive, either alone or in combination, in the sense that a third party (such as a police officer) having access to it could result in harm to the person involved. For example, some of the information – such as photographs from criminal records – may suggest what someone's race or ethnicity is, while other data may be suggestive of poverty or financial difficulty. We are not suggesting that companies intend for police to misuse their systems to make decisions based on

109 See, e.g., General Services Administration, Procurement identifiers DJA14AHDQP0887 (September 26, 2014 – January 5, 2018), 15A00018PAQ00519 (May 28, 2019); 15A00022PAQA00298 (July 21, 2022 – August 20, 2025); all viewable at fpds.gov.

110 Human Rights Watch, Dark Side: *Secret Origins of Evidence in US Criminal Cases,* January 9, 2018, https://www.hrw.org/report/2018/01/09/dark-side/secret-origins-evidence-us-criminal-cases (accessed September 17, 2025).

race, class or other inappropriate factors; indeed, it is possible that such behaviors would breach some companies' terms of service, and some databases may contain protections of which we are not aware. Additionally, in the US, it is lawful to collect and share potentially sensitive personal data, including about characteristics such as race and income, in most circumstances. (See above for a more detailed discussion of existing legal restrictions.) However, it is our view that without strong safeguards established in law, police could misuse such data based on bias.

In addition to sensitivity concerns, there is no guarantee that the information data brokers offer to police is accurate. At least some of the brokers we examined explicitly acknowledge the risk of inaccuracy in disclaimers;[111] however, based on the cases below, we see a risk that officers will believe in the reliability of information from databases in spite of disclaimers and, at times, even in circumstances where information from other sources contradicts what they are seeing on the screen.

Police using these systems can often view data not only about the person standing before them or passing by in a car, but also the person's spouse, other family members, neighbors, and "associates." One Accurint document formerly available on the LexisNexis Risk Solutions website posited that an officer responding to a call should know "who is at the scene" before arriving, "as the resident may have potentially dangerous relatives or associates" and as other people living at the address may have "associated criminal records."[112] For us, such statements prompt concerns about potential profiling by police that could lead to biased actions or unnecessary uses of force, even though we do not believe this is what the companies intend (and many might deplore such behaviors). For example, if police responding to a call for help at a house look up the address and see that someone living there was once accused of a crime, will they be more likely to approach with their guns drawn?

In marketing these large data collections (or the ability to merge such collections) to law enforcement, we have found instances in which companies have used language that we believe risks reinforcing biases against poor people and minorities. A marketing document for data analysis platform seller SAS has claimed that the company's systems enable "preventative policing" that "helps break the cycle of offending that can run in families" – language that we think risks reinforcing longstanding racial and class-based stereotypes, or could encourage presumptions of guilt based on people's associations, although we are not claiming that this is

111 For example, LexisNexis has stated in a user guide for Accurint LE Plus: "Accurint data is updated routinely from various contributing sources, both publicly and commercially available. These sources can contain errors and are generally not totally free from defect. This system should not be considered definitively accurate and all data should be independently verified before taking any action based on the results." LexisNexis, "Accurint LE Plus: Accurint for Law Enforcement Plus User's Guide," 2019, p. 2 (*supra,* n. 108). See also LexisNexis, "Accurint LE Plus", https://risk.lexisnexis.com/products/accurint-le-plus (accessed September 17, 2025): "Due to the nature of the origin of public record information, the public records and commercially available data sources used in reports may contain errors. Source data is sometimes reported or entered inaccurately, processed poorly or incorrectly, and is generally not free from defect. This product or service aggregates and reports data, as provided by the public records and commercially available data sources, and is not the source of the data, nor is it a comprehensive compilation of the data. Before relying on any data, it should be independently verified."

112 LexisNexis, "White Paper: Closing the Case: Solving Violent Crimes Quickly and Efficiently with Public Records," January 2010, pp. 3-4, formerly available for download at https://risk.lexisnexis.com/products/accurint-for-law-enforcement (last accessed May 10, 2024; a version is viewable at https://web.archive.org/web/20180905100713/https://risk.lexisnexis.com/-/media/files/government/white-paper/closing-the-case-pdf.pdf).

what the company intended.[113] The Accurint promotional document mentioned above, published in 2010, promoted the idea that people experiencing poverty or financial instability are unusually likely to commit crimes, remarking on an "economic downturn" and suggesting that increasing numbers of people might "commit crime to financially survive"—even while conceding that violent crime rates had been decreasing or stable for years.[114]

Meanwhile, several of the marketing materials we examined touted the money companies say police departments can save by performing database lookups. A 2011 Accurint promotional document provided cost breakdowns for three situations in which, according to LexisNexis, instant access to personal data through the system resulted or could have resulted in hundreds or thousands of dollars in savings to departments searching for suspects.[115] Thomson Reuters has advertised its CLEAR database to police departments as able to mitigate the impact of "deep budget cuts."[116] TransUnion, owner of TLOxp, says law enforcement should "turn to TLOxp to achieve more economical, effective and timely results."[117]

Police, however, should not seek cost savings at the expense of human rights. Cheap data access, while legal under US law, may tempt officers to dive into large collections of personal information when other investigative methods would have been more appropriate or accurate. It may also lead to unnecessary and potentially harmful investigations of "associates" whose connection with a suspect or the location of a crime is weak or irrelevant.

Additionally, police with easy access to privately held personal data could misuse it to carry out many of the same harms this report documents regarding access to government-held data, such as stalking and other sexual or gender-based harms.

113 SAS, "How police forces can use data to prevent crime," https://www.sas.com/en_us/insights/articles/risk-fraud/how-police-use-data-to-prevent-crime.html (accessed August 21, 2019).

114 LexisNexis, "White Paper: Closing the Case: Solving Violent Crimes Quickly and Efficiently with Public Records," p. 2.

115 LexisNexis, "Case Study: LexisNexis Accurint for Law Enforcement," 2011, pp. 2, 3-4, 6 (downloaded from https://risk.lexisnexis.com/products/accurint-for-law-enforcement circa 2019 and on file with the authors).

116 Thomson Reuters, "CLEAR for law enforcement," https://legal.thomsonreuters.com/en/products/clear-investigation-software/law-enforcement#b (accessed September 17, 2025).

117 TransUnion, "How Law Enforcement Can Speed Up Investigations," July 22, 2025, https://www.transunion.com/blog/law-enforcement-speed-up-investigations (accessed September 17, 2025).

ii. Types of personal data for sale to US police

a. Address, contact information, and Social Security numbers

Data brokers offer police instant access to extensive information about people's current and past addresses, phone numbers, and other contact and identifying information. This information could easily amount to a record of everywhere a person has ever lived and every phone number they have ever had.

Utility companies appear to be one major source of contact information that data brokers buy. To receive electricity, gas, and other basic services necessary to life in a modern house or apartment, US customers typically must provide their names and contact information. While few people in the country likely realize that this data can be sold to data brokers and then to police, a TransUnion document accessed through our research in 2019 stated that TLOxp's "Utility Search Module allows you to search nationwide for people based on utility connections and disconnects, such as TV, Internet & Cable, Cellular, Local & Long Distance Phone Lines, Water, Gas, and Electricity."[118] Thomson Reuters has similarly claimed that its CLEAR database offers information "from more than 70 utilities nationwide, including electric, gas, satellite, water, fuel oil, and other utilities."[119]

Some data brokers flag addresses, phones, and Social Security numbers as suspicious or present them in a way that we believe could imply wrongdoing such as identity theft, despite disclaimers. For example, a user guide for Accurint LE Plus has stated that this system for law enforcement has shown yellow check marks to suggest that there are "Risk Indicators" associated with a person's address or phone number.[120] Officers who read the guide would have discovered that "Risk indicators—in and of themselves—are not necessarily indicators of fraud or of any fraudulent intent."[121] However, we are concerned that indicators of this kind may invite police suspicions or judgments in practice. The user guide we found does not disclose what information would have caused the database to flag an address or phone number as somehow connected with risk, and it is unclear whether officers using the system may have had access to any information on this point.

118 TransUnion, "TLOxp User Tips," 2015, p. 25, https://tloxp.tlo.com/docs/People_Search_User_Tips.pdf (accessed August 21, 2019 and now on file with the authors).

119 Thomson Reuters, "Thomson Reuters CLEAR: The Smarter Way to Get Your Investigative Facts Straight," 2015, p. 5, accessed September 17, 2025, and archived version available at https://web.archive.org/web/20250716212952/https://www.thomsonreuters.com/content/dam/openweb/documents/pdf/legal/fact-sheet/clear-brochure.pdf.

120 LexisNexis, "Accurint LE Plus: Accurint for Law Enforcement Plus User's Guide," *supra* n. 108, pp. 51, 63.

121 Ibid.

At least two of the major databases we examined have also flagged Social Security numbers as potentially problematic.[122] Social Security numbers are often used in the US to verify people's identities, including in financial and other highly sensitive contexts, and crimes of fraud can entail the use of a fictitious Social Security number or one belonging to someone else. Therefore, we are concerned that data seeming to suggest an individual may have used multiple or incorrect Social Security numbers – particularly without an explanation of the origins of this data and whether it may be inaccurate – could raise officers' suspicions that the person has committed a crime or is dishonest, even if the information is accompanied by prominent disclaimers.

While data such as addresses, phone numbers, and Social Security numbers may seem relatively innocuous, especially in the hands of authorized police users, we are of the view that they hand a great deal of power to officers in reality—including the tools to make biased assumptions about whether people have a propensity for committing crimes, along with a practical ability for officers to stalk, harass, or impersonate individuals.

b. Photographs, information about race or ethnicity, and facial recognition

The information data brokers offer to police about people may include photographs from a variety of sources, such as criminal records and social media profiles; we infer that these photographs may be suggestive of race or ethnicity, at least at times, as race in the US is a social category typically constructed on physical appearance (for example, skin color).[123] Data integration platforms, too, may prominently feature photographs and information about race.[124]

Some data brokers have also begun offering facial recognition data to law enforcement. Most famously, a company called Clearview AI has gained law enforcement customers in the US – and continues actively pitching its product to federal agencies – after having amassed a vast database of photographs of people from social media and other sources. The company positions its facial recognition technology as a time- and money-saving measure for police, but has attracted controversy and legal actions in a number of jurisdictions, including both the US and UK,[125] over

122 LexisNexis, "Accurint LE Plus: Accurint for Law Enforcement Plus User's Guide," *supra* n. 108, p. 63 (reference to "SSN Risk Indicators"); Thomson Reuters, "Thomson Reuters CLEAR: The Smarter Way to Get Your Investigative Facts Straight," *supra* n. 119, p. 3 ("Multiple SSNs," "SSN Matches multiple individuals," "SSN Recorded as Deceased," "Age Younger than SSN Issue Date")

123 See, e.g., LexisNexis, "Accurint LE Plus: Accurint for Law Enforcement Plus User's Guide," (*supra* n. 108), pp. 11, 158-159.

124 See, e.g., SAS, "SAS Criminal Justice Data Integration and Analytics," p. 2, accessed August 29, 2019 and archived at https://web.archive.org/web/20151002235505/https://www.sas.com/content/dam/SAS/en_us/doc/factsheet/criminal-justice-data-integration-analytics-106602.pdf; the sample profile on p.2 of the PDF appears to include a drop-down menu for "Race," along with photographs and mock results that include descriptors of "Race."

125 Privacy International, "Challenge against Clearview AI in Europe" https://privacyinternational.org/legal-action/challenge-against-clearview-ai-europe (accessed 2 December 2025).

its alleged privacy impact.[126] (At the time of writing, the company had stated its intention to appeal an October 2025 ruling from the UK Upper Tribunal confirming that its processing is subject to the GDPR[127]).) Accurint has also claimed to have an "Image Matching" feature.[128]

Facial recognition raises a wide range of human rights concerns, including the risk that police may use it to identify and investigate people whom they have no other reason to suspect of any wrongdoing, or engage in abuses such as harassment or stalking. Facial recognition also raises specific concerns about potential rights harms to minorities, since studies have shown that historically, several such systems have been less accurate for people of color and women than for light-skinned men.[129]

Even searchable databases that simply contain photographs – without facial recognition technologies – raise concerns, as they could give officers instant but unnecessary access to information about someone's race, gender or other characteristics that could give rise to discrimination. For example, an officer who looks up the license plate number of a passing car could see information about the driver's race even if the officer did not see the driver. We are concerned that the availability of unnecessary data about people's characteristics, particularly race, could prompt police decisions based on bias.

c. Family members, neighbors, and associates

Based on our research, it appears that data brokers often provide police with data not only about the person who is the subject of the lookup, but people the broker has designated as connected with that person.

In Accurint, this data may include information about a purported spouse—including that person's "Workplace Name, Address, and Phone Number."[130] It may also include information belonging to people who live in the same building as the person of interest, other neighbors, relatives, and "[a]

126 Kashmir Hill, "The Secretive Company That Might End Privacy as We Know It," New York Times, January 18, 2020, https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html (accessed September 17, 2025); Clearview AI, "Unlocking the Power of Facial Recognition in Criminal Investigations," https://www.clearview.ai/criminal-investigations (accessed September 17, 2025); Clearview AI, "The Power of Facial Recognition in U.S. Federal Government," https://www.clearview.ai/federal (accessed September 17, 2025); Taylor Hatmaker, "Clearview AI banned from selling its facial recognition software to most US companies," TechCrunch, May 9, 2022, https://techcrunch.com/2022/05/09/clearview-settlement-bipa/ (accessed September 17, 2025);

127 Privacy International, "Tribunal Confirms Clearview AI Bound by GDPR" (October 13, 2025) https://privacyinternational.org/news-analysis/5692/tribunal-confirms-clearview-ai-bound-gdpr (accessed 2 December 2025); Clifford Chance, "ICO v Clearview AI: The reach of GDPR and the breadth of 'behavioural monitoring'" (October 23, 2025) https://www.cliffordchance.com/insights/resources/blogs/regulatory-investigations-financial-crime-insights/2025/10/the-reach-of-gdpr-and-the-readth-of-behavioural-monitoring.html (accessed 2 December 2025).

128 LexisNexis, "LexisNexis Accurint Virtual Crime Center," https://risk.lexisnexis.com/products/accurint-virtual-crime-center (accessed September 17, 2025).

129 See, e.g., Steve Lohr, "Facial Recognition Is Accurate, if You're a White Guy," *New York Times*, February 9, 2018, https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html (accessed September 17, 2025).

130 LexisNexis, "Accurint LE Plus: Accurint for Law Enforcement Plus User's Guide," p. 53 (*supra* n. 108).

ssociates" of a person or place.[131] TransUnion has similarly said TLOxp displays "1st, 2nd, & 3rd Degree Relatives['] Phone Numbers" and ages, as well as "Neighbor Phones" and "Likely" and "Possible Associates."[132]

Several companies have said they offer information not only about individuals and – based on simple connections – relatives and associates, but complex analytics to create detailed maps of family, personal, and professional relationships.

For example, Accurint parent company LexisNexis has sold access to a "link analysis" system called Relavint, which the company said allows officers to draw links "between individuals and their relatives, associates, addresses, vehicles, corporations, and other items."[133] Similarly, TLOxp has offered "Relationship Reports" that the company has advertised as containing a "visual graph" including detailed connections between "subjects, businesses and more."[134]

Such tools raise a concern for us that people may become objects of law enforcement suspicion simply because of who their family members or neighbors are, with a potential impact on the freedom of association—a human right.

d. Vehicles and automated license plate reader data

Car ownership is common in the United States, many areas of which lack comprehensive public transportation systems. Data brokers that sell information to police often offer information about the cars associated with a person (and vice versa), as well as data from drivers' licenses. For example, Accurint has said it enables police to conduct "wildcard" searches that can identify people the database associates with a full or partial license plate number or type of car. In a hypothetical instance, "you can run a query to find all red Fords within a State, which have a 'D' as the second character in the tag," the company has stated in a user guide.[135]

Having information about a car's license plate may also enable a data broker to report on people's past locations, thanks to automated license plate reader (ALPR) technology. Motorola, for example, has said it offers both fixed and car-mounted license place recognition cameras, along with software, to scan license plate numbers—creating a record of where cars have been. The company appears to scan license plates against a database of potentially stolen or, perhaps, otherwise suspicious vehicles or people, generating more than 1 million "[d]aily hot list alerts."[136]

Police can purchase access to ALPR data directly from such entities, while some other data brokers say they also buy access to such data and present it to law enforcement alongside the other information they hold about a person.[137]

---

131 Ibid. at pp. 31-32, 53, 75.

132 TransUnion, "TLOxp User Tips," p. 54.

133 Lexis Nexis, "Relavint Desktop," https://www.accurint.com/relavintdesktop.html (accessed September 17, 2025).

134 TransUnion, "TruLookup Relationship Mapping," https://www.transunion.com/solution/trulookup/investigate-alert/relationship-mapping (accessed September 17, 2025).

135 LexisNexis, "Accurint LE Plus: Accurint for Law Enforcement Plus User's Guide," pp. 103, 111 (*supra* n. 108).

136 Motorola Solutions, "License Plate Recognition," https://www.motorolasolutions.com/en_us/video-security-access-control/license-plate-recognition-camera-systems.html (accessed September 17, 2025).

137 See, e.g., Thomson Reuters, "CLEAR License Plate Recognition," https://legal.thomsonreuters.com/en/c/thomson-reuters-clear-license-plate-recognition (accessed February 5, 2026).

By contrast, police use of a physical GPS device they have surreptitiously attached to a car would require a warrant, under a 2012 US Supreme Court opinion.[138]

Location tracking, including via ALPRs, can be highly revealing of a person's private life: for example, where they worship, which health care facilities they visit, where they shop or drink or gamble, and whom they drive to see in the middle of the night. We are concerned that suspicionless identification of drivers via ALPRs could also lead to needless encounters with police, akin to occurrences in some of the cases described below—and that such needless encounters could be dangerous for both the driver and the officer.

e. Social media data

Some data brokers market their systems to police on the basis of their ability to mine data from social media websites. TLOxp, for example, has offered a product that searches for publicly posted social media material associated with a person, allowing police to "[i]nvestigate behaviors of a subject based on their online (public-facing) posting activity" and "discover new associates or subjects of interest."[139] People-search site Spokeo has prominently featured its access to social media information in its online promotional materials for law enforcement, saying it provides officers with data from "120+" social media networks. Such data includes "geotagged posts and photos" that can potentially reveal a person's location, as well as "friend and family connections" and "associates' addresses" (language that was current as of 2024).[140] As of 2019, the company said it was "partnering with the intelligence community," and specifically highlighted its ability to gather data from Facebook, Instagram, YouTube, Twitter, Amazon, Skype, LinkedIn, dating sites Tinder and OKCupid, television and video streaming sites, and the shopping sites eBay and Etsy, among scores of other platforms.[141] (The relevant promotional page on its website has since changed.)

In response to our request for comment, Spokeo stated that it "collects only publicly available information from public sources, including phone books, social networks, marketing surveys, real estate listings, business websites, and other public sources ('Public Information')," and asserted that it "has long been a leader in making it easy for consumers to opt-out and suppress their Public Information from display on Spokeo.com," including via a "self-service opt-out tool" available to all, regardless of where the data subject resides.[142]

---

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

139 TransUnion, "Every Subject Has a Digital Story. TruLookup Social Media Search Can Help Tell Them All," 2023, https://www.transunion.com/content/dam/tlo/us/documents/DM-23%20F127323%20SRV%20Q1%202023_Asset%20Sheet%20-%20TLOxp%20Social%20Media%20Report.pdf (accessed September 17, 2025).

140 Spokeo, "Spokeo for Law Enforcement," https://www.spokeo.com/law-enforcement (accessed May 14, 2024); archived version available at https://web.archive.org/web/20240501123141/https://www.spokeo.com/business/law-enforcement?g=law_direct_landing.

141 The main researcher for this report viewed the page on August 22, 2019. See https://web.archive.org/web/20180805055945/https://www.spokeo.com/law-enforcement, showing the page as it appeared in 2018, with the icons of "social media platforms searched." The website changed at some point prior to May 21, 2021.

142 Email from Chief Legal Officer, Spokeo, to Privacy International, 31 January 2026 (on file with the authors).

Babel Street, which has been another prominent client of governments and police forces worldwide, has marketed a "PAI Solution" (PAI standing for "publicly available information") that, the company has said, performs AI-driven data analytics on the "ocean of data" created by people and devices every day. The tool seems to go further than providing a structured database of PAI: the company says it is designed help clients determine the relevance of individual data points and "view them through a lens that joins and reviews all data sources to meet your objective".[143] The tool also seems to collect data that is not readily available to the average internet user even if that data is, or has been, "public" in some sense.[144]

While people often post information about themselves on social media websites voluntarily and publicly, we view companies' collection and storage of this information, and sale of the data to police, as raising numerous rights concerns. First, although users might be expected to know that police could view their public posts, the copying, storage, and mining en masse of those posts by police – potentially for years or decades – may have distinct consequences for privacy. The UN High Commissioner for Human Rights has recognized this problem, stating that "when information that is publicly available about an individual on social media is collected and analysed, it also implicates the right to privacy. The public sharing of information does not render its substance unprotected."[145]

Second, there are few laws that govern these activities by police and set limits to ensure respect for rights.

Third, it appears to us that data brokers could draw inferences from people's social media information – such as conclusions about race or income level – that are inaccurate; we are also concerned that in practice, police could misuse such information in a way that is discriminatory.

Lastly, we are concerned that the lack of legal limits on constant aggregation or monitoring of social media data by police or data brokers could ultimately discourage lawful free expression and free association online to an extent that violates human rights.

f. Employment and finances

Many data brokers offer information about a person's employment, assets, and financial history to US law enforcement. According to Accurint, such information can "reveal evidence of financial distress or prior criminal activities."[146] Access to this information, like all data broker information discussed in this Section, does not require a warrant, court order, or subpoena. That is, without needing to show any probable cause or other reason to believe an individual has committed a crime, police have the legal ability to view data that they may interpret as suggesting a propensity or motive to engage in wrongdoing.

---

143 Babel Street, "Publicly Available Information Explained," https://www.babelstreet.com/blog/pai-explained (accessed September 17, 2025).

144 Ibid; Babel Street, "Three Keys to Staying Ahead of Risk Using PAI," https://www.babelstreet.com/blog/3-keys-to-staying-ahead-of-risk-using-pai (accessed October 10, 2025).

145 Report of the UN High Commissioner for Human Rights, Rights to privacy in the digital age, UN doc. A/HRC/29/39, para. 6.

146 LexisNexis, "Accurint for Law Enforcement," https://risk.lexisnexis.com/products/accurint-for-law-enforcement (accessed September 17, 2025) (see drop-down text under "Quickly Uncover Assets"; the same phrase also appears on a page titled "Accurint for Government").

A sample Spokeo report for police about a fictitious person, which has been available for several years, includes an explicit "Wealth" information category. The report estimates the fictitious person's household income based on data from marketers, provides the value of his home, and lists his current and previous employers and job titles.[147]

iii. Does this happen elsewhere in the world?

The US may not be an isolated case. Law enforcement agencies elsewhere may very well be purchasing access to data brokers' databases, although such practices haven't been as clearly reported in other countries.

In the UK, our searches of the public procurement database ContractsFinder.service.gov.uk produced very few relevant results. Still, a few are concerning. Notably, Experian (a leading international credit referencing agency with associated data broking services) has said it offers a service in the UK called "Investigator Online" that "provides Police and Law enforcement agencies with instant on-line access to Experian's data and insights."[148] Freedom-of-information requests have revealed that this service has been used by at least the Staffordshire Police[149] and Bedfordshire Police,[150] under a framework agreement made between Experian and the Police and Crime Commissioner for Nottinghamshire. Nottinghamshire Police Force have also contracted Experian under the header of "Experian for Crime", likely under the same framework.[151] A 2023 freedom-of-information request unrelated to our research has revealed that between 2021 and the date of the request (which is unclear), London's Metropolitan Police Service spent more than £1.5 million (approximately $1.8 million US) on information from Experian and £1.2 million (approximately $1.5 million US) on information from Equifax, and has also purchased data from TransUnion.[152]

147 Spokeo, "William Matthew Foster, Age 33," https://www.spokeo.com/pdf/sample-report.pdf (accessed August 22, 2019 and September 17, 2025).

148 Experian, "Locate the right individual with real-time access to Experians IOL" (Service definition document, 2021), available from https://www.applytosupply.digitalmarketplace.service.gov.uk/g-cloud/services/485058705009061 (accessed September 17, 2025).

149 Staffordshire Police, Fire and Crime Commissioner, "Use of Third Party Data Services," (response to FOI request SCO/FOI/033/2024), 13 December 2024, https://www.whatdotheyknow.com/request/use_of_third_party_data_services (accessed September 17, 2025).

150 Though note that this information was provided in a response by Hertfordshire Constabulary; Hertfordshire Constabulary, "Use of Third Party Data Services," (response to FOI request FOI2024/04421), 30 July 2024, https://www.whatdotheyknow.com/request/use_of_third_party_data_services_2 (accessed September 17, 2025). This appears to be because Hertfordshire, Bedfordshire and Cambridgeshire share resources in an information unit.

151 Nottinghamshire Police Force, "Experian For Crime," 29 April 2019, https://www.contractsfinder.service.gov.uk/notice/45eb8293-14fe-4abf-a8d7-e5dd7857c38a?origin=SearchResults&p=1 (accessed September 17, 2025).

152 Metropolitan Police, "Purchasing information from data brokers" (response to FOI request 01.FOI.23.032792), https://www.met.police.uk/foi-ai/metropolitan-police/disclosure-2024/january-2024/purchasing-information-data-brokers/.

IV. Law Enforcement Misuse of Large Collections of Personal Data Today

"To say that the investigation … was sloppy is being kind."

This Part includes discussions of sexual and gender-related abuse, and alleged race-based mistreatment, that some readers may find disturbing.

Our review of 130 federal civil lawsuits filed since 2011, along with other relevant cases, establishes a history of serious law enforcement abuse of access to large collections of personal data and shows that the risk of harm is real.

In multiple instances, police have used incorrect information in databases in ways that have resulted in people being wrongly arrested or detained – in some cases for days, months, or years. As discussed above, there is no guarantee that information about people in these large databases is accurate, and we conclude that police should be fully aware of the potential for inaccuracy by now.

At other times, police have used information in databases that is correct, but have done so in what we regard as abusive or illogical ways that have resulted in investigations or detentions of people without any clear factual reason to suspect them of wrongdoing. In many cases, people of color have been the victims of this type of abuse, or of judgment calls that erred on the side of suspicion and force. For example, one officer's decision to look up someone in a database without any reasonable suspicion of wrongdoing became a contributing factor in the man's death. In another case, an officer's apparently inaccurate use of database information contributed to a shooting incident in a man's home. In 2021, police in Los Angeles looked up the license plate of a vehicle simply because it was a "nice grey BMW" being driven in Skid Row; the officers then interpreted the database results as indicating that the vehicle might be stolen – disregarding other database records indicating that the license plate was not associated with any reported theft – and carried out a "high risk" traffic stop involving a total of 13 police on the ground, drawn firearms, and helicopter backup. As in many such cases, the driver was Black – and, according to the complaint, a military veteran with post-traumatic stress disorder.[153]

Police have also looked up information about women with no law enforcement justification, including in the context of stalking and sexual violence. Some of these women have been their fellow officers, public safety personnel, or criminal justice professionals.

At times, police have allegedly looked up local political candidates or officials, according to a small number of the cases we examined.

153 *Augustus v. City of Los Angeles et al.*, Order Granting in Part Defendants' Motion for Summary Judgment and Granting Plaintiff's Motion for Summary Judgment (doc. 97), case no. 2:22-cv-02640 (C.D. Cal.), May 31, 2023, pp. 1-4; *Augustus v. City of Los Angeles et al.*, Complaint (doc. 1), case no. 2:22-cv-02640 (C.D. Cal.), April 20, 2022, pp. 4-11. The parties "dispute[d] the extent to which the officers pointed their guns directly at" the driver (doc. 97, p.3 at fn. 3).

In court filings, statements made under oath, and interviews we conducted as part of this research, victims of police misuse of personal data from large databases have described serious harms. (Owing to lengthy delays between the interviews and the publication of this report, we have chosen not to publish the interviews, but they have informed our analysis.) Some of the harms they claim to have experienced, such as sexual assault, may rise to the level of cruel, inhuman, or degrading treatment or punishment, which is universally banned under the Convention against Torture. Other harms they have alleged, such as jailing or imprisonment in difficult conditions on the basis of mistaken identity – which victims have described as a deeply disturbing experience – may also rise to this level, on top of potentially amounting to wrongful imprisonment (a violation of the right to liberty under international human rights law). In interviews and depositions, victims have further described harms to dignity, mental health, family life, educational progress, and careers. We have not sought to prove these claims, but regard them as consistent and serious enough to indicate that lawmakers should not simply wave them aside.

Yet, in many of the cases described below, courts have not held officers, their departments, or local governments accountable. In many instances, this result emerged because the judges in these cases found that officers could claim "qualified immunity," which – according to a line of US cases beginning in the late 1960s – protects police and other local officials from being held liable in civil rights lawsuits unless they have violated a constitutional right that was clearly established at the time and about which "a reasonable person would have known."[154]

This position stands in stark contrast with the jurisprudence of other countries and international human rights institutions such as that of the European Court of Human Rights, which holds all state authorities to account and does not recognize immunity for violations of people's rights.

Following the murder of George Floyd by Minneapolis Police Department officers and resulting protests in 2020, many civil rights groups and activists in the US, along with local, state, and federal legislators, have called for laws that would end qualified immunity, and by the summer of 2020, the cause had widespread public support.[155] In an exceptionally critical decision from the US District Court for the Southern District of Mississippi in a lawsuit brought by a Black man whom police pulled over even though their search of a law enforcement database gave rise to no cause for concern, the judge decried qualified immunity as a doctrine that US courts had "invented … to protect law enforcement officers from having to face any consequences for wrongdoing." He added, "In real life it operates like absolute immunity."[156]

---

154 *Harlow v. Fitzgerald*, 457 U.S. 800, 818 (1982). On the history and breadth of qualified immunity, see generally Congressional Research Service, "Policing the Police: Qualified Immunity and Considerations for Congress," February 21, 2023, available at https://crsreports.congress.gov/product/pdf/LSB/LSB10492 (accessed October 1, 2024).

155 See, e.g., Kimberly Kindy, "Dozens of states have tried to end qualified immunity. Police officers and unions helped beat nearly every bill," *Washington Post*, October 7, 2021, https://www.washingtonpost.com/politics/qualified-immunity-police-lobbying-state-legislatures/2021/10/06/60e546bc-0cdf-11ec-aea1-42a8138f132a_story.html (accessed October 1, 2024); Pew Research Center, "Majority of Public Favors Giving Civilians the Power to Sue Police Officers for Misconduct," July 9, 2020, https://www.pewresearch.org/politics/2020/07/09/majority-of-public-favors-giving-civilians-the-power-to-sue-police-officers-for-misconduct/ (accessed October 1, 2024).

156 *Jamison v. McClendon*, Order Granting Qualified Immunity (doc. 72), 476 F.Supp.3d 386, 391, case no. 3:16-CV-595 (S.D. Miss.), August 4, 2020, p. 5.

However, notwithstanding the re-introduction of a bill in the US Congress to restrict qualified immunity in early 2023, reform efforts are currently stalled.[157]

Victims of police harms in the US can file civil rights claims not only against individual officers, but also their departments and local governments. However, under US law, police departments and municipal entities are also immune from suit unless an action is unconstitutional and "implements or executes a policy statement, ordinance, regulation, or decision officially adopted and promulgated by [the] body's officers."[158]

Plaintiffs therefore face high hurdles in obtaining redress for police abuses of their personal data: they must prove that a right is clearly established in US law and that an officer reasonably should have known that she or he was violating it – or that a police department's action was both unconstitutional and carried out as a matter of policy or official decision. In practice, these standards have deprived plaintiffs of remedies – even where, as a federal district court opined in 2019 in a case stemming from police database use resulting in an arrest based on mistaken identity, "[t]o say that the investigation … was sloppy is being kind."[159]

157 See Office of Ed Markey, "Markey, Pressley Announce Legislation to End Qualified Immunity," April 19, 2023, https://www.markey.senate.gov/news/press-releases/markey-pressley-announce-legislation-to-end-qualified-immunity (accessed October 1, 2024); Kimberly Kindy, "Dozens of states have tried to end qualified immunity. Police officers and unions helped beat nearly every bill," *Washington Post*, October 7, 2021, https://www.washingtonpost.com/politics/qualified-immunity-police-lobbying-state-legislatures/2021/10/06/60e546bc-0cdf-11ec-aea1-42a8138f132a_story.html (accessed October 1, 2024).

158 *Monell v. Department of Social Services,* 436 U.S. 658, 690 (1978).

159 *Nerio v. Evans et al.*, case no. 1:17-cv-00037 (W.D. Tex.), Report and Recommendation of the United States Magistrate Judge (doc. 41), June 19, 2019, p. 15. The Court of Appeal in this case was less harsh in its description of the officers' decisions during the investigation, concluding that the misidentification involved was a "reasonable" mistake. *Nerio v. Evans et al.*, case no. 19-50793 (5th Cir.), Judgment, September 10, 2020, p. 7.

A. Mistaken identity

Many of the people wrongly arrested in these cases had to wait days, months, or even years to be released.

Nathaniel Maybin, Jr. did not assault a man with a hammer near a Philadelphia deli in 2014. But thanks in part to the way they carried out database searches, police believed he did – and this incorrect belief had dire consequences for Maybin.[160]

Maybin's story illustrates one of the problems arising from insufficient limits on police access to large collections of personal data. This is mistaken identity: the misidentification of one person as another, or as matching a suspect's description, as a result of information in a database. In cases we examined, such mistakes often appear to have had devastating consequences for the people affected.

As one US legal scholar has observed, "Arrests[] triggered by database access can have life-changing negative consequences for those targeted." The scholar adds that in addition to the "traumatic experience" of the arrest and detention themselves – which will often entail strip searches, blood and DNA sample collection, and other intrusions on the body and privacy – the criminal records generated by an arrest "have a self-replicating effect on the streets." This is because they provide police with "new bases to stop, question, search and even arrest individuals, fueling continued criminal justice system contacts."[161]

In the cases below, officers often appear to have acted based on confirmation bias: information they saw in databases led them to believe that a certain person was the perpetrator, even when there were few or no other reasons to believe the person was linked to any crime. The officers

160 *Maybin v. Slobodian et al.*, case no. 2:16-cv-01394 (E.D. Pa.), Memorandum Opinion (doc. 23), September 28, 2017.

161 Logan, "Policing Police Access to Criminal Justice Data," pp. 640-641, 645-646, 655.

then discarded or ignored information that contradicted their belief in the person's guilt. In some instances, the available records show disturbingly few indications that officers cared whether they had arrested the correct person. In other cases, the records show an obvious risk of mistakes

stemming from something as simple and preventable as a mis-click: one man was arrested in 2015 after a court clerk selected the wrong "Matthew S. Smith" from a drop-down menu when issuing a warrant.[162]

Newer cases raise the possibility that this confirmation bias operates mainly in one direction: officers who have viewed database results that (in their opinion) indicate that someone has a criminal record or may be involved in a crime often are not dissuaded by information contradicting these suspicions. By contrast, when a database search comes up clean or clearly contradicts the officers' beliefs, officers may well disregard this information and continue to pursue their line of action.[163]

In other words, having a "bad" digital record linked to your name – even wrongly – can hurt you, but having a "good" or "clean" digital record linked to your name (or information that distances you from the alleged crime) will not necessarily help you.

Many of the people wrongly arrested in these cases had to wait days, months or even years to be released, enduring a Kafkaesque situation in which they protested their innocence and sought to establish their real identities to no avail – sometimes resulting in lasting psychological harm, they have said. Some, such as Maybin and M.R., might have been imprisoned or detained for even longer if not for luck or helpful connections.

We are concerned that due to apparently widespread and uncorrected database errors; the fact that police do not need any individualized suspicion, let alone a court order, before searching large databases; and the potential for officers' confirmation bias or disregard of the risk of a wrongful arrest, everyone in the United States is at risk of having their lives upended through such mistakes.

We are also concerned that the trauma and other harms of these events may be magnified for people who endure the distress of insisting that police have arrested the wrong person – while being dismissed or ignored.

---

162 *Smith v. Finch et al.*, Statement of Material Uncontested Facts (doc. 93), case no. 1:18-CV-00118 (E.D. Missouri), July 17, 2018, pp. 4-6; *Smith v. Finch et al.*, Memorandum and Order (doc. 110), December 18, 2018, p. 5 (uses phrase "drop-down menu").

163 See, e.g., *Gill v. Magan et al.*, case no. 2:19-cv-00860 (W.D. Wa.), Order on Motion for Summary Judgment (doc. 81), March 11, 2021, pp. 3-4. We note that following the trial in this civil case, the jury found in favor of the defendants. *Gill v. Magan et al.*, Jury Verdict (doc. 144), May 5, 2021. The Court of Appeal upheld various aspects of the trial following an appeal by *Gill, Gill v. City of Seattle* 2:19-cv-00860 (9th Cir.), Memorandum (doc. 173), September 29, 2022.

Nathaniel Maybin

Nathaniel Maybin, whom a video recording showed at a Chinese restaurant miles away from the scene just minutes before the assault took place, spent more than 17 months in detention before his acquittal and release in 2015.

According to court records, in February 2014, a man was "brutally assaulted" while walking to a deli in West Philadelphia, and police who arrived at the scene found a mobile telephone nearby.[164]

A detective later stated that he performed a "Clear" database search for information about the phone's number, and that the results indicated that the number belonged to "Maybin, N." (Court records do not confirm whether this was a search of Thomson Reuters' CLEAR database, although the opinion appears to suggest this, describing the system as one "used by officers to look up subscribers of phone numbers.") The detective then found database information for Nathaniel Maybin, Sr., a middle-aged man. However, a witness had described the suspect as being approximately 25 to 30 years old.[165]

Instead of concluding that the phone's owner and the perpetrator of the assault might be different people (or using an established formal process to request records from the telephone company that could have identified the phone number's subscriber more clearly), the detective carried out database searches to find other people who might be "N. Maybin." The logic behind this decision to check large databases for other "N. Maybins" is unclear. However, these further database searches led the detective to Nathaniel Maybin, Jr., a 28-year-old Black man (and the son of Nathaniel Maybin, Sr.).[166]

The detectives investigating the assault believed that some of Maybin, Jr.'s characteristics and his photograph in the database were similar to witnesses' descriptions of the suspect. For this reason, a detective included a photo of Maybin, Jr. in a photo line-up with several other people, and two witnesses then separately identified him as the perpetrator.[167]

The problem is that neither Maybin, Jr. nor Maybin, Sr. had anything to do with the crime.

---

164 *Maybin v. Slobodian et al.*, case no. 2:16-cv-01394 (E.D. Pa.), Memorandum Opinion (doc. 23), September 28, 2017, pp. 1-2.

165 Ibid., pp. 2-3 and fn. 2; *Maybin v. Slobodian et al.*, Oral Deposition of Detective Dennis Slobodian, Exhibit A to Defendants' Memorandum of Law in Support of Motion for Summary Judgment (doc. 21-1), filed February 15, 2017, pp. 22-23.

166 *Maybin v. Slobodian et al.*, Memorandum Opinion (doc. 23), pp. 2-3; Oral Deposition of Detective Dennis Slobodian (doc. 21-1), pp. 22-23, 26-27.

167 *Maybin v. Slobodian et al.*, Memorandum Opinion (doc. 23), pp. 2-3; Oral Deposition of Detective Dennis Slobodian (doc. 21-1), pp. 24, 26-27.

According to Maybin and later testimony by a detective, Maybin's father tried to tell the police that the phone found at the scene of the assault belonged to him (the father) and that he had simply lost it on the day of the crime. However, officers – the court later wrote – "concluded he was lying."[168]

Maybin was arrested and placed in detention. His bail was set at one million dollars, which he and his loved ones could not afford to pay.

At trial, the defense introduced a videotape showing Maybin at a Chinese restaurant miles away from the scene just minutes before the assault. Maybin was acquitted in 2015 and released after spending more than 17 months in jail.[169]

If not for the lucky development regarding the videotape, Maybin may have been sentenced to further years or decades in prison for a crime he did not commit.

The acquittal has not erased the erroneous linking of Maybin to the crime in the public eye. His name continues to appear online in news reports from the time of the assault bearing headlines such as "Suspect in West Philadelphia hammer attack held on $1 million bail."[170]

The federal trial court dismissed Maybin's civil suit alleging false arrest and malicious prosecution on grounds including a finding that the database results, together with other information, had been sufficient to establish probable cause for Maybin's arrest.[171] The Court of Appeals for the Third Circuit upheld the dismissal of the case.[172]

Though the courts did not grant Maybin any relief in his case, another court ruling on a case similar to his came to a different conclusion. As part of the federal prosecution of a California man in 2013, a court found that an "Accurint record that [the suspect's] phone number was 'associated' with" an address was not sufficient to establish for policing purposes that the man lived at the location. The court in that case noted that "at the hearing government counsel could not explain to the court what this 'association' means" and, for this reason in combination with others, ruled that a warrant that had been issued for a search of the residence was not based on probable cause to believe evidence of a crime would be found there – and was therefore unconstitutional.[173]

168 *Maybin v. Slobodian et al.*, Memorandum Opinion (doc. 23), pp. 3-4; Oral Deposition of Detective Dennis Slobodian (doc. 21-1), pp. 33-36.

169 *Maybin v. Slobodian et al.*, Memorandum Opinion (doc. 23), at *8.

170 "Suspect in West Philadelphia hammer attack held on $1 million bail," 6 ABC Action News, February 26, 2014, https://6abc.com/archive/9445044/ (accessed October 1, 2024).

171 *Maybin v. Slobodian et al.*, Memorandum Opinion (doc. 23), at *12-13.

172 *Maybin v. Slobodian et al.*, 739 F. Appx. 161, case no. 17-3316 (3d Cir. 2018).

173 *United States v. Mitchel*l, 2013 U.S. Dist. LEXIS 138975 (N.D. Cal.), Order Granting Motion to Suppress, September 26, 2013, pp. *2, 6-7.

M.R.

"I really thought, I'm never going home. I'm going to have a birthday in jail. I'm not going to be there for my niece's first birthday a week after that. I'm not going to see my kids for a while."

In another case, bad personal data that had persisted in databases for five years resulted in an arrest and detention based on mistaken identity.

While driving with her young daughter in the eastern United States during a shopping trip one afternoon in 2015, a woman we are calling "M.R." was followed and then pulled over by a state trooper (i.e., police officer).[174] The trooper had searched the state's law enforcement database, and by extension information from NCIC, for M.R's license plate number while in his patrol car.[175] The system produced results suggesting that M.R.'s vehicle belonged to someone with a similar name who was the subject of a 2009 bench warrant.[176] (Bench warrants are issued for people who have failed to appear for proceedings and have been held in contempt of court.) The other woman had a different middle name, a surname that was spelled slightly differently, and (M.R. alleged) a recorded weight that differed from M.R.'s by 100 pounds. (The district court ultimately acknowledged a weight discrepancy but found that it was not of critical significance to the case).[177]

When the warrant was issued, it appears that police had inadvertently linked data about M.R. to data about the accused woman; this bad data then persisted in the state's database and NCIC for years.[178] The state trooper arrested M.R. – over her protests – and she was immediately taken to prison, where she was detained for 48 hours.[179] We note here that the court, in describing these alleged circumstances, took pains to state that it was not making findings of fact and that it had construed the evidence in the light most favorable to M.R., as it was required to do at that stage of the proceedings.[180]

174 Documentation on file with the authors. While the person's name is part of the public record, we have anonymized the details of this case in our report due to the medical nature of some of the personal information we discuss.

175 Documentation on file with the authors.

176 Documentation on file with the authors.

177 Documentation on file with the authors.

178 Documentation on file with the authors.

179 Documentation on file with the authors.

180 Documentation on file with the authors.

M.R. later brought a federal civil rights lawsuit, arguing that officers had clearly violated her rights by arresting and imprisoning her based on a warrant that had been issued for someone else; however, the officers and other relevant officials denied that any rights violations had taken place, and the court dismissed M.R.'s case on grounds that included qualified immunity in 2020.[181]

We include M.R.'s case here in part because of her deposition, which makes the point that being detained in a Kafkaesque situation of mistaken identity – including because of a database error – could lead to humiliation and serious distress even if the authorities ultimately realize they have detained the wrong person. Although her civil rights lawsuit never reached the stage where M.R.'s claims about both the immediate and lasting psychological consequences of her detention would have been tested in court (and we assume that the defendants would have disputed them), she described a range of such consequences. According to her, these included psychological difficulties during the initial traffic stop: a sensation of sickness to her stomach as the trooper followed her car, a sense of unreality after she was pulled over and told there was a warrant for her arrest, and confusion during the ensuing encounter.[182] She also described alleged aspects of the booking and imprisonment procedure that, even if common, could still be emotionally disturbing: being compelled to use the bathroom with the door open; being pressed against a wall for a pat-down search; having her bra removed and cut up in front of her; experiencing a feeling of panic; being belittled by a male prison staff member; anxiety serious enough to warrant medication.[183] (We offer a reminder here that these claims were not proven in court.)

The consequences of the mistaken arrest and imprisonment were lasting, M.R. claimed in her deposition: she described carrying extra documentation with her in case anyone ever felt motivated to question her identity again, quitting her job due to anxiety provoked by the incident, feeling withdrawn, having a persistent sense of self-doubt, sleeplessness, disproportionate anger, and a reluctance to leave the house. She expressed a sense of no longer liking her own name and of no longer being the same person.[184]

181 Documentation on file with the authors.

182 Documentation on file with the authors.

183 Documentation on file with the authors.

184 Documentation on file with the authors.

H.W.

"What kind of world is this that you ... go and ride in your car, and because somebody has the same name you have, you're going to go to jail?"

A traffic stop and database search led to events similar to those described in M.R.'s suit in a different eastern US state in early 2014, when an officer looked up a car's license plate in a police database and received results indicating that a warrant was linked with the vehicle's registration. The officer then determined that the car was owned by a woman we are calling "H.W.," who was also a passenger that day. The warrant had been issued for someone with the same name.

The H.W. in the car, who was legally blind and had previously suffered a stroke, maintains she protested to the officer and said there was no reason to arrest her (something the government later disputed). However, the officer handcuffed her and removed her to a detention facility. H.W., who is Black, was detained for about two hours until – she alleged – authorities determined that the warrant had been issued for a different woman who was white and twenty years younger. (The authorities disputed these claims about the differences between H.W. and the woman listed in the warrant.) She was then detained for another two hours before being released.[185]

During a deposition in the resulting lawsuit, an attorney for the government asked H.W. if she felt better knowing that the events in question had happened because of mistaken identity. H.W. replied:

"Absolutely not. It makes me feel worse, and I'm going to tell you why: Because what kind of world is this that you cannot go and ride in your car, and because somebody has the same name you have, you're going to go to jail. There should be some way to distinguish that I'm not that person....

If it was set up like that, all of us would be in jail at any given time, fighting to get out [because] it's not us. It's unconstitutional, and it's violating. It's violating people. [The officer] violated me in the worst possible way.

... I live my life in the right way, and I respect law officers. He has put a real damper on my opinion. I should not have to be afraid to approach a police officer for fear that it's going to be flipped back on me, and he's done that." [186]

The federal court rejected H.W.'s lawsuit on the grounds that the arrest had been reasonable, since the database showed that a warrant had been issued for someone with H.W.'s name.[187]

185 Case name withheld due to inclusion of health information. The court opinion from which the description of this incident is drawn is a public record and is on file with the authors.

186 Deposition on file with the authors.

187 Opinion on file with the authors.

Jose Vasquez

Jose Vasquez has alleged that in 2016 and 2017, he was repeatedly and wrongly arrested for homicide by officers in Washington, DC, based on NCIC information allegedly linking Vasquez to an Illinois warrant that was nearly 40 years old and had been issued for someone else. [188]

For years, the complaint maintains, "Plaintiff Vasquez lived in constant fear of being re-arrested for a crime he never committed in a state in which he has never set foot."[189] At least twice, he was detained following traffic stops – once for 10 days – and threatened with extradition to Illinois.[190]

Following a trial in 2022, a jury found the city liable for false imprisonment and awarded Vasquez $100,000 in compensatory damages.[191] Washington, DC's Metropolitan Police Department has denied violating Vasquez's rights, and in 2023, the district court overturned the jury verdict on the grounds that the evidence was not sufficient to support it.[192] The federal appeals court overturned the district court's decision in this respect in 2024, and the jury award was reinstated.[193]

188 *Vasquez v. District of Columbia et al.*, case no. 1:17-cv-02194 (D.D.C.), Second Amended Complaint (doc. 40), November 28, 2018; Memorandum Opinion and Order (doc. 96), September 30, 2021, pp. 2-3.

189 *Vasquez v. District of Columbia et al.*, Second Amended Complaint (doc. 40), ¶ 2.

190 *Vasquez v. District of Columbia et al.*, Memorandum Opinion and Order (doc. 96), pp. 3-5.

191 *Vasquez v. District of Columbia et al.*, Jury Verdict (doc. 121), May 12, 2022.

192 *Vasquez v. District of Columbia et al.*, Memorandum Opinion (doc. 132), March 29, 2023.

193 *Vasquez v. District of Columbia et al.*., case no. 23-7050 (D.C. Cir.), Opinion of the Court (doc. 2069176), August 9, 2024; *Vasquez v. District of Columbia et al.*, case no. 1:17-cv-02194 (D.D.C.), Judgment (doc. 142), September 23, 2024.

Reginald Smith

Similarly, a city government's alleged failure to correct the personal data associated with a bench warrant, as well as an alleged practice of linking "alias" names to the warrants, led to a 2011 lawsuit in California. Reginald Smith, a Black man, claimed to have been arrested in Tennessee and extradited to Los Angeles in 2007 based on mistaken identity. He claimed to have been detained again in 2011 due to a continuing failure to de-link his database information from the warrant record in question.[194]

Smith's complaint raised the possibility that the entry of "alias" names into criminal justice databases – for example, because suspects have allegedly used various names – can cause warrants to be linked to innocent people, meaning that the correction of any erroneous information can be crucial to avoiding mistaken arrests. The defendants in this civil suit issued blanket denials of Smith's allegations, as is common at this stage of US federal proceedings, and the court did not reach the stage of weighing the alleged facts; the case ended in a settlement in 2015.[195]

194 *Smith v. County of Los Angeles et al.*, case no. 2:11-cv-10666 (C.D. Cal.), Fourth Amended Class Action Complaint for Injunctive Relief and Damages (doc. 150), April 21, 2015, ¶¶ 53-65.

195 *Smith v. County of Los Angeles et al.*, Answer of Defendants County of Los Angeles and Los Angeles County Sheriff's Department to Plaintiff's Fourth Amended Complaint (doc. 153), May 5, 2015, ¶¶ 1, 7 *et seq.*; Answer of Defendant Barbara Fryer to Plaintiff's Fourth Amended Complaint (doc. 163), June 4, 2015, ¶¶ 1, 5 *et seq.*; Mediation Report (doc. 166), June 24, 2015.

Melissa Neylon

"Alias" names were also at issue in a case brought by California resident Melissa Neylon.

When Neylon completed an employment-related form at a county jail in late 2015, a search of the California Law Enforcement Telecommunications System (CLETS) database using her date of birth and her maiden name, Melissa Smith, produced results indicating that an Indiana court had issued a warrant for someone named Melissa Chapman. According to the database, Chapman was suspected of identity theft, and had previously used the name "Melissa Smith" along with other names by which Neylon had been known during earlier marriages.[196] Fingerprint records did not link Neylon to Chapman, instead linking Neylon only to her own previous names. Yet, Neylon was detained for two weeks, until additional fingerprint information confirmed that she was not the wanted person.[197]

Like H.W., M.R. and others, Neylon protested that she was not the person named in the warrant – but, she later said, she was disbelieved and ignored. (The defendants denied many of the facts Neylon alleged.)[198] Whether police ever considered the possibility that the database could be mistaken is unknown.

According to Neylon in the lawsuit she later filed, officials had also disregarded other disparities between the descriptions of her and Chapman, including differences between Neylon's description of herself as of mixed race and records describing Chapman as white.[199] The court nevertheless dismissed Neylon's lawsuit, finding that similarities between the two women were sufficient to "support a good faith and reasonable belief" that Neylon was Chapman, and that the arrest was therefore justified.[200]

196 *Neylon v. County of Inyo et al.*, case no. 1:16-cv-00712 (E.D. Cal.), Order on Defendant's Motion for Summary Judgment and Order on Plaintiffs' Motion to Amend (doc. 84), August 3, 2018, pp. 3-4.

197 Ibid., pp. 5-9.

198 Ibid., pp. 5-6; regarding the defendants' denials, see generally *Neylon v. County of Inyo et al.*, Amended Answer to Plaintiffs' Fourth Amended Complaint and Demand for Jury Trial (doc. 66), September 7, 2017.

199 *Neylon v. County of Inyo et al.*, Order on Defendant's Motion for Summary Judgment and Order on Plaintiffs' Motion to Amend (doc. 84), pp. 10, 12.

200 Ibid., pp. 12-13.

Indigo Hatcher

Indigo Hatcher had the misfortune of being someone whose photograph was stored in a police database. According to her deposition, she was also a college athlete and a volunteer at a local high school.[201]

An officer in Jersey City, New Jersey was watching a vacant lot one December afternoon in 2014 when he observed a suspected drug sale involving two women who eventually entered a nearby house. At the police station, the officer asked a detective to search a law enforcement database containing information about people who had previously been arrested. The database searches returned a photograph of Hatcher, a Black woman, among other information. Upon viewing the image, the officer decided Hatcher was the woman he had seen and obtained a warrant for her arrest.[202]

Hatcher, however, had an alibi, she testified in her deposition: her employer's records showed she had been at work in a different city that afternoon.[203] (The defendants appear to have disputed this alibi, or at least its relevance).[204] In 2015, prosecutors dropped the charges against her, admitting that her arrest had resulted from mistaken identity.[205] The lawsuit resulted in a settlement in early 2020.[206]

---

201 *Hatcher v. City of Jersey City Police Department et al.*, case no. 2:2015-cv-08303 (D.N.J.), Plaintiff's Statement of Material Facts (doc. 57-1), May 17, 2018, p. 1.

202 *Hatcher v. City of Jersey City Police Department et al.*, Opinion (doc. 63), February 27, 2019, pp. 2-5. Hatcher's complaint suggests that Hatcher and the suspects were Black. Hatcher v. City of Jersey City Police Department et al., Complaint (doc. 1), November 25, 2015, p. 3. See also Deposition of Dejon Morris (doc. 35-17), filed March 31, 2017, p. 10.

203 *Hatcher v. City of Jersey City Police Department et al.*, Plaintiff's Statement of Material Facts (doc. 57-1), May 17, 2018, p. 1.

204 *Hatcher v. City of Jersey City Police Department et al.*, Defendants' Statement of Relevant Undisputed Material Facts in Support of Motion for Summary Judgment (doc. 35-1), March 31, 2017.

205 *Hatcher v. City of Jersey City Police Department et al.*, Opinion (doc. 63). at pp. 5-6; Memorandum in Opposition to Plaintiff's Motion to Compel Production of Grand Jury Minutes (doc 44), June 1, 2017, p. 1.

206 *Hatcher v. City of Jersey City Police Department et al.*., Order of Dismissal (doc. 80), February 27, 2020.

Gerardo Espinosa Guerra

Like Indigo Hatcher, Gerardo Espinosa Guerra of Georgia said he became the victim of a chain of events that began with faulty assumptions based on information in a database and ended with an officer incorrectly deciding, based on a photograph, that he was a suspect the officer had seen. Unlike Hatcher, Guerra had become aware of the potential for such an error regarding his identity, and he had proactively provided local authorities with identity documents to establish who he was.[207] It did not matter: police ultimately detained him for 16 days, although they later denied wrongdoing.[208]

Guerra's eventual lawsuit alleged that in early 2015, following an episode at a Tennessee hotel, local police obtained a warrant for the arrest of one Gerardo Emmanuel Espinosa Zamudio; it was later agreed among the parties that this warrant appeared in the NCIC database.[209] Nine months later, in a Georgia city nearly 300 miles away, local officers appeared at Gerardo Espinosa Guerra's home to speak with his stepfather. (Note the difference in the names.) Guerra later claimed that while resolving the officers' inquiry, he provided them with his driver's license (something the defendants neither admitted nor denied).[210] It was later agreed that the officers then entered Guerra's name into NCIC, generating a "hit" – apparently one linked to the warrant for Zamudio.[211] However, they let Guerra go, allegedly upon learning that Guerra had tattoos while Zamudio did not.[212]

As everyone later agreed, Guerra then voluntarily appeared at the local sheriff's office and provided personal information such as his Social Security number and driver's license in an effort to explain that he was not the person sought in the Tennessee warrant.[213]

Nevertheless, police in Georgia then sent a photograph of Guerra to police in Tennessee to find out if Guerra was a wanted person there.[214] The Tennessee detective who received the photograph showed it to another officer, who said "that's him" – that is, that Guerra was the suspect they were looking for.[215] The two police forces then arranged for Guerra to be arrested on the Tennessee warrant.[216]

---

207 *Guerra v. Rockdale County, Georgia et al.*, case no. 1:16-cv-04656 (N.D. Ga.), Amended Complaint for Damages (doc. 33), August 14, 2017, p. 14; Answer to Amended Complaint (doc. 35), August 28, 2017, pp. 10; see generally denials of wrongdoing throughout the Answer to Amended Complaint.

208 *Guerra v. Rockdale County, Georgia et al.*, Amended Complaint for Damages, p. 24; Answer to Amended Complaint, p. 17.

209 *Guerra v. Rockdale County, Georgia et al.*, Amended Complaint for Damages, pp. 9-12; Answer to Amended Complaint, p. 8.

210 *Guerra v. Rockdale County, Georgia et al.*, Amended Complaint for Damages, p. 13; Answer to Amended Complaint, p. 9.

211 *Guerra v. Rockdale County, Georgia et al.*, Answer to Amended Complaint, p. 8.

212 *Guerra v. Rockdale County, Georgia et al.*, Amended Complaint, pp. 13-14.

213 *Guerra v. Rockdale County, Georgia et al.,* Amended Complaint, p. 14; Answer to Amended Complaint, pp. 10-11.

214 *Guerra v. Rockdale County, Georgia et al.,* Answer to Amended Complaint, p. 11.

215 *Guerra v. Rockdale County, Georgia et al.,* Amended Complaint, pp. 15-17; Answer to Amended Complaint, pp. 11-13.

216 *Guerra v. Rockdale County, Georgia et al.,* Amended Complaint, pp. 18-19; Answer to Amended Complaint, pp. 14-16.

According to Guerra's later complaint, the arrest and detention occurred even though Guerra and Zamudio "had different full names, different addresses, different phone numbers, different body markings, different social security numbers, different residence statuses, as [Guerra] is a citizen and Zamudio is undocumented," and even though the police in Tennessee had a photograph of Zamudio. (The defendants neither admitted nor denied these allegations, although they denied behaving unlawfully.)[217]

Thus, Guerra – who had done nothing wrong, and had proactively sought to prove his identity – sat in detention for 16 days, accused of being a fugitive from justice and, according to his later complaint, "suffer[ing] the anxiety, stress, and humiliation of facing prosecution for heinous crimes he did not commit."[218]

The federal district court partly dismissed the case, including on grounds that a reasonable officer in Georgia "could have believed that probable cause existed to arrest" Guerra, resulting in a lack of a constitutional violation; regarding the Tennessee police, the court dismissed the claims on grounds that included qualified immunity.[219] The parties agreed to a dismissal of the remainder of the case in 2020; it is not clear whether this agreement followed a settlement.[220]

217 *Guerra v. Rockdale County, Georgia et al.,* Amended Complaint, pp. 24-25; Answer to Amended Complaint, pp. 18, 20 et seq.

218 *Guerra v. Rockdale County, Georgia et al.,* Amended Complaint, p. 24; Answer to Amended Complaint, p. 17

219 *Guerra v. Rockdale County, Georgia et al.,* Opinion and Order (doc. 60), October 28, 2019, pp. 12 et seq

220 *Guerra v. Rockdale County, Georgia et al.,* Stipulation of Dismissal with Prejudice (doc. 98), August 12, 2020

John Newsome

"Nothing I said made one bit of difference to them about me being innocent."

Photographs were also at issue in a mistaken identity case in Newark, New Jersey, that arose after five assailants, including two men, attacked a man near his apartment above a daycare center in 2011.

The victim believed the perpetrators worked at the daycare center, although he only knew the name of one.[221] An officer searched various police databases for photographs of people matching the descriptions the victim had given, but with one exception, the victim was unable to confirm that any of the photographs depicted his attackers.[222]

The officer then entered the daycare's address into Accurint, which returned search results linking multiple people to the address; one of these people was a woman for whom the system recorded a 2006-era connection.[223] According to Accurint, by 2011 the woman was living 96 miles away with a man named John Newsome.[224]

The officer took the names of every male on the list that Accurint generated, cross-referenced them with DMV record photos, and showed them to the victim as the system returned them. When the photo of Newsome appeared, the victim identified him as the other male attacker.[225] Newsome was arrested at work in November 2011, after which police learned that his wife's father owned the building where the day care was located.[226] Police had evidently decided that Newsome was a suspect based on this tenuous connection in a database between Newsome and the day care's address.

Newsome was held in jail for four days before he could make bail, and in February 2012 was indicted for the assault.[227] After the victim ultimately retracted his identification of Newsome as the assailant, the charges were dropped.[228]

---

221 *Newsome v. City of Newark et al.*, case no. 2:13-cv-06234 (D. N.J.), Opinion (doc. 89), August 31, 2017, pp. 1-2.

222 Ibid. at p. 2.

223 Ibid. at p. 3 and 6; *Newsome v. City of Newark et al.*, Statement of Undisputed Material Facts (Defense) (doc. 71-2), October 7, 2016, p. 5; Exhibit E (doc. 71-8), October 7, 2016, p. 11.

224 *Newsome v. City of Newark et al.*, Opinion (doc. 89), p. 3; see also Exhibit E (doc 71-8), p. 11.

225 *Newsome v. City of Newark et al.*, Opinion (doc. 89), p. 3; Statement of Undisputed Material Facts (Defense), pp. 5-6.

226 *Newsome v. City of Newark et al.*, Opinion (doc. 89), p. 6

227 Ibid. at p. 6

228 Ibid. at p. 8; *Newsome v. City of Newark et al.*, Statement of Undisputed Material Facts (Defense) (doc. 71-2), p 12.

Asked by one of the defendants' attorneys about the distress these events had caused him, Newsome described:

"Straight-up embarrassment from the day they walked into that Social Security office [where the arrest occurred] and put those handcuffs on me and escorted me outside there and put me in the car.

Printed ... in the newspaper that I was charged for five felonies....

The fact that nothing I said [after the arrest] made one bit of difference to them about me being innocent....

The fact that they offered me six-and-a-half years in prison." [229]

The federal court in New Jersey that heard Newsome's case ruled that the police had been reasonable in concluding that there was probable cause to believe that Newsome was the perpetrator, and it further ruled that Newsome therefore had not been deprived of clearly established constitutional rights when he was arrested. The court granted summary judgment in favor of the defendants.[230]

229 *Newsome v. City of Newark et al.*, Deposition of John Anthony Newsome (doc 71-11), filed October 7, 2016, pp. 19-20.

230 Ibid. at pp. 9-10, 34.

Cornell McKay

In a case with similarities to Newsome's, information police discovered using a "TLO search" contributed to Cornell McKay's prosecution and ultimate conviction for robbery of a cell phone and $50 in Missouri in August 2012. The "TLO search" linked one of the numbers someone dialed from the phone after it was stolen to an address, and thus to a person associated with the address.[231] According to the information before the court at the pre-trial stage, additional "computer searches" led to the identification of that person's "associates," including Cornell McKay – the only one of the associates who police said fit the description the victim had provided of the person who robbed her.[232] McKay was therefore several degrees removed from any direct connection with the stolen phone.

Nevertheless, police included a photograph of McKay, who is Black, in a photographic lineup and the victim identified McKay as the person who robbed her. McKay was soon arrested despite his claims of an alibi.[233] Police and prosecutors appear to have ignored other evidence that undermined the likelihood that McKay had committed the robbery when choosing to indict and prosecute him, such as several connections that emerged between the stolen phone and one Keith Esters, later convicted of a murder during an attempted robbery in the same area and carried out in a manner similar to that McKay was accused of perpetrating.[234]

At his trial in December 2013, McKay was convicted and sentenced to 12 years in prison, although in 2014, an appellate court vacated this conviction, finding that the lower court should not have excluded evidence related to Esters. Prosecutors wanted to retry McKay, but the robbery victim did not wish to testify, prompting the state to drop the charges. By then, McKay had been detained or imprisoned for nearly three years, both on the charges and on a supposed probation violation resulting from arrest for alleged crime.[235]

---

231 *McKay v. City of St. Louis, Missouri et al.*, case no. 4:15-cv-01315 (E.D. Mo.), Memorandum and Order (doc. 238), March 31, 2019, pp. 2-3.

232 Ibid., p. 3.

233 Ibid., pp. 3-4.

234 Ibid., pp. 4-5; Danny Wicentowski, "Keith Esters, Megan Boken's Killer, Has Nothing to Say About Cornell McKay", *St. Louis Metro News*, May 19, 2015, https://www.riverfronttimes.com/news/keith-esters-megan-bokens-killer-has-nothing-to-say-about-cornell-mckay-2771961 (accessed October 17, 2024; archived version available at https://web.archive.org/web/20240810005752/https://www.riverfronttimes.com/news/keith-esters-megan-bokens-killer-has-nothing-to-say-about-cornell-mckay-2771961).

235 *McKay v. City of St. Louis, Missouri et al.*, Memorandum and Order (doc. 238), pp. 4-5.

After his release, McKay sued law enforcement for violation of his constitutional rights. A federal court opined that law enforcement's investigation and prosecution were "not perfect"; that there was substantial credible evidence that Esters, not McKay committed the robbery; and that the officers' judgment may have been "flawed, even negligent." However, the court also found that the conduct alleged did not meet the high standard of "intentional or reckless" behavior that "shocks the conscience" required for relief. It therefore dismissed the complaint against the defendant officers and police department in 2019.[236] The federal appeals court affirmed the dismissal of the case in 2020.[237]

236 Ibid., pp. 19, 35-36 and discussions passim.

237 *McKay v. City of St. Louis, Missouri et al.*, Opinion (8th Cir. E.D. Mo.), June 4, 2020.

Patrick Moore

Officers in Joliet, Illinois obtained a phone number they believed they could call to arrange a purchase of crack cocaine, and subsequently set up a videotaped undercover purchase of the drug for $50 in 2010.[238] On the day he planned to buy the drug, an officer searched Accurint to find information about the phone number's subscriber, and the database suggested the number belonged to a man named Patrick Moore. The officer then found a photograph and physical description of Moore in police and state databases, compared these with the videotape of the undercover drug buy, and decided Moore was the person on the tape.[239]

The problem, a federal judge later determined, was that Moore's photograph didn't actually bear much resemblance to the man in the videotape: both images showed "young, black males with short hair," but otherwise – in the judge's view – the resemblance was weak. "Not only is their general appearance noticeably different, but several specific features stand out," the judge wrote, listing perceived differences in skin tone, eyebrows, mouth shape, hairline, and cheekbones.[240] To the judge, the two images viewed side-by-side "immediately" raised questions about whether the officer had identified the right suspect.[241]

Without the image connection, the only significant evidence purportedly linking Moore to the crime was the database result linking his name to the phone number police had used to set up the controlled drug buy: not enough proof, in the judge's view, to justify an arrest.[242]

The state ultimately dismissed the charges against Moore—but not until he had spent approximately five months in detention.[243] Moore's civil lawsuit resulted in a settlement in late 2015.[244]

238 *Moore v. Banas et al.*, case no. 1:11-cv-05654 (N.D. Ill.), Memorandum Opinion and Order (doc. 101), September 23, 2015, pp. 1-2. The description of events in this case reflects facts the court described as undisputed. Ibid. at p. 2.

239 Ibid. at pp. 2-3.

240 Ibid. at pp. 5-6.

241 Ibid. at p. 5 (quoting *Maxwell v. City of Indianapolis*, 998 F.2d 431, 434 (7th Cir. 1993)).

242 Ibid. at pp. 6-7.

243 Ibid. at p. 3; *Moore v. Banas et al.*, Amended Memorandum of Law in Support of Summary Judgment (doc. 71), May 29, 2014, p. 6.

244 *Moore v. Banas et al.*, Notification of Docket Entry (doc. 103), November 25, 2015.

Jane Doe, a 14-year-old

Thanks in part to personal information in a database, US authorities perceived a Black child from Texas, who has said she spoke no Spanish, as an adult woman from Colombia and removed her from the country.

In dismissing a civil rights complaint brought by a young Black US girl in 2013, a federal judge in Texas characterized the case as concerning "a fourteen year old who intentionally and consistently provided a false name to local Houston law enforcement officers and thereafter to immigration authorities under oath."[245]

However, we believe it is also possible to view the case as illustrating an obvious risk of police searches for information about children or other people with a diminished ability to make reasoned decisions. If the database information is wrong, a child or someone else who has difficulty understanding the potential consequences of their actions may not try to correct the mistake – especially if they are frightened, or if they think their situations will be better if everyone believes they are someone else. We also see this case as potentially illustrating a risk that a child who is frightened or has recently survived trauma may even persist in telling a story that aligns with what the database has suggested, despite disastrous repercussions.

According to a civil rights complaint later filed by the girl and her mother, Jane Doe—while in mourning for her grandfather—was "lured away from her home by a child predator," trafficked to Houston, and subjected to physical and sexual abuse.[246] The complaint maintained that after Doe ran away from the trafficker, she "was conflicted by feelings of shame and guilt associated with the untoward activities that she had unwillingly participated in," and – not realizing that she had been victimized – feared that her family would be angry with her.[247] (These claims were not tested in court, as a judge dismissed the case at an early stage.)

The complaint went on to allege that when Doe (still missing) was eventually arrested for shoplifting in Houston in 2011, she made a fateful mistake: she gave the officers a false name. Unfortunately, the name Doe – a US citizen – chose was apparently associated in a law enforcement database with a Colombian woman in her early twenties who was suspected of being an undocumented immigrant.[248]

---

245 *Turner v. U.S. et al.*, case no. 4:13-cv-00932 (S.D. Tex.), Memorandum and Order (doc. 23), October 31, 2013, p. 1. The "Turner" of the case title is Jane Doe's mother; Jane Doe is anonymized in the case record, and we follow suit, although some media coverage has not done so.

246 *Turner v. U.S. et al.*, Complaint (doc. 1), April 2, 2013, pp. 7-8.

247 Ibid. at pp. 8-9.

248 Ibid. at pp. 8-9; *Turner v. U.S. et al.*, Memorandum and Order (doc. 23), pp. 3-4.

Doe persisted in the untruth, and it appears that officers accepted her story: less than two months after her arrest for shoplifting, she was deported to Bogotá, where – her complaint alleged – she remained for seven months in an extremely vulnerable state, experiencing further sexual abuse and a pregnancy.[249]

In other words, the complaint alleged that thanks in part to a connection in a database, US authorities perceived a Black American child from Texas, who has said she spoke no Spanish,[250] as an adult woman from Colombia and removed her from the country.

In comments to the media after Doe and her mother filed their civil rights lawsuit, ICE blamed the child for "consistently us[ing] a false identity with her dealings with the Houston police, her defense attorney, ICE, the immigration court and the Colombian government."[251] Doe and her mother alleged that ICE failed to carry out a fingerprint analysis or other database searches that could have disproven the supposed link between the teenager and the allegedly undocumented immigrant woman.[252]

Doe's situation highlights a recurring issue in the cases we have reviewed: since access to these databases is only provided to the police, suspects or defendants in mistaken identity cases and their lawyers do not stand a fair chance of reviewing the information accessed by the police, at least until trial. Even then, they often will not have a way to compel the government or a company to change records that are incorrect or misleading.

The federal judge in Texas dismissed Doe's lawsuit on the grounds that it would be improper for her to receive a remedy, since she had misled officers by repeatedly claiming a false identity.[253]

249 *Turner v. U.S. et al.*, Complaint (doc. 1), pp. 13-14. Press coverage suggests that the US government has not disputed that the deportation occurred: see Juan Carlos Llorca and Linda Stewart Bell, "Texas teen deported to Colombia reunites with mom", *Associated Press*, January 7, 2012, https://apnews.com/article/texas-colombia-immigration-ce46e908a83d4bbdad1ee54a2344d38d (accessed October 17, 2024).

250 *Turner v. U.S. et al.*, Memorandum and Order (doc. 23), p. 6.

251 Cameron Langford, "U.S. Teen Deported, Spends Seven Months in Colombia," *Courthouse News Service*, May 25, 2012, https://www.courthousenews.com/u-s-teen-deported-spendsseven-months-in-colombia/ (accessed October 17, 2024; quote also available at https://www.cbsnews.com/texas/news/mom-of-deported-dallas-teen-runaway-files-suit/).

252 *Turner v. U.S. et al.*, Memorandum and Order (doc. 23), p. 5.

253 Ibid. at pp. 18-21.

Andrew Carr

"It is undisputed that the search of Plaintiff's residence resulted in a surprising and dangerous invasion of his proper[t]y that was not instigated by any wrongdoing on his part."

In Ohio in 2016, a SWAT team detonated a "flash bang" device and entered Andrew Carr's Ohio home to arrest a suspect, M.M., who they believed lived there based on information contained in police databases. However M.M. no longer resided at the address, and police were "aware that there were also other possible residences" for him, as a federal court later explained.[254]

Carr, who was not a suspect in the investigation of M.M., fired a shot at the door as the officers entered his home, and as a result was arrested and detained for five months for allegedly assaulting a police officer. (Carr later maintained that the officers had not announced themselves, although the police disputed this.) The state ultimately dropped the criminal charges against Carr.[255]

Carr complained in his civil lawsuit that, as a result of these events, he had incurred thousands of dollars in legal fees while defending himself from the criminal charges, lost his employment, and was unable to be sworn in as a US citizen, as he said he had been scheduled to do on the day of the raid.[256]

The federal court presiding over the lawsuit concluded, "It is undisputed that the search of Plaintiff's residence resulted in a surprising and dangerous invasion of his proper[t]y that was not instigated by any wrongdoing on his part." However, the court found that there was "no evidence to suggest" that the officers' actions "were anything other than reasonable, warranted, and properly authorized," and it therefore dismissed Carr's claims.[257]

254 *Carr v. Johnson et al.*, case no. 1:17-cv-00620 (N.D. Ohio 2018), Memorandum Opinion (doc. 82), December 13, 2018, pp. 2-3. Although we have found sources dating to the early 2000s that mention a Factual Analysis Criminal Threat Solutions database, we have been unable to determine the nature of this database.

255 Ibid. at p. 3.

256 *Carr v. Johnson et al.*, Complaint (doc. 1), March 24, 2017, paras. 65-67.

257 *Carr v. Johnson et al.*, Memorandum Opinion (doc. 82), pp. 18-19.

Nancy Gill

"Alone, terrified, and without any connection to crimes"

In a 2017 case similar to Carr's, Nancy Gill was at home in Lake Stevens, Washington, drying her hair when officers from the Seattle Police Department "broke down [her] front door" and arrested her with guns drawn. Gill, the district court later said, was "alone, terrified, and without any connection to crimes." Officers had burst through her door in search of someone else—a male suspect whom they believed was living with his mother. Gill, however, was only nine years older than the suspect, meaning that she could not be his mother.[258]

Unlike in Carr's case, officers appear to have disregarded information in a database (Accurint) indicating that it was Gill – and not the suspect or his mother – who lived at the relevant address. Instead, they relied on information in other databases and from other sources.[259]

In 2021, Gill's case against the officers overcame the hurdle of qualified immunity; however, the jury found in favor of the defendants following a trial shortly afterward.[260] The Court of Appeal upheld this result following an appeal by Gill.[261]

258 *Gill v. Magan et al.*, case no. 2:19-cv-00860 (W.D. Wash), Order on Motion for Summary Judgment and Motion to Exclude (doc. 81), March 11, 2021, pp. 2-5.

259 Ibid.

260 Ibid.; *Gill v. Magan et al.*, Jury Verdict (doc. 144), May 5, 2021.

261 *Gill v. City of Seattle* 2:19-cv-00860 (9th Cir.), Memorandum (doc. 173), September 29, 2022.

What went wrong

These cases highlight police officers' reliance on information in large databases accessible to them without a warrant—information that is often incorrect, unclear, outdated, or contradictory, with harmful results that include the arrest, detention and imprisonment of innocent people. Some of the encounters have involved drawn firearms, with all the dangers inherent in such a scenario.

Several of the cases suggest to us that officers may be too quick to assume that database information is necessarily correct or relevant, and more inclined to believe database information than other evidence, or claims of real identity or innocence offered by the person they have detained; we are concerned that officers may even be inclined to view digitized information as inherently reliable and persons encountered in the course of their duties as inherently unreliable. While there is an obvious risk that suspects will lie about their identities, these cases show there is also a risk that innocent people will be arrested, detained, and even prosecuted.

In our opinion, some of the cases also suggest that confirmation bias – the long-documented psychological tendency to prefer information that supports a belief one already holds – may be a risk when officers view database information about people before carrying out other investigative steps. In other words, officers who view database information may unconsciously begin to seek out or discard other evidence based on whether it confirms what they have already seen in the database results.

Some of the cases raise serious questions about the necessity of widespread instant access to law enforcement information about relatively minor offenses or other records of encounters with the criminal justice system. For example, in the M.R. suit described above, the trooper had instant access from his patrol car to information about an alleged minor fraud – access that does not seem essential to highway policing, and that resulted in real harm when the information turned out to be wrong.

In other instances, as in the cases of Maybin and Newsome, the apparent rush to identify and arrest a suspect led to database-inspired leaps of logic, the flaws of which – we believe – should have been obvious. Newsome's and McKay's cases also involved a practice of singling out suspects from databases based on how closely the person matches a witness' description of the alleged perpetrator, then including the person's photograph in a lineup – with little or no other evidence to tie the person to the scene of the crime. These cases suggest that such an approach to investigations can result in serious mistakes.

In several of these cases, police overvalued minimal database information or remote links to the location of an offense, seemingly treating this information as compelling evidence of culpability. In two of these cases involving people of color, officials or courts also displayed (or allegedly displayed) a willingness to discount information indicating that the actual suspect was white. Those cases involved disputed chains of events, and we can only know what we see in the court documents, which necessarily provide only a limited picture of the circumstances and cannot reveal the officers' or judges' states of mind. However, we believe the question of how judges and police may be treating contradictory information about race in investigations involving the use of databases would be worth exploring at a systemic level.

Courts dismissed several of the cases described above without any finding that the alleged victims were entitled to restitution, potentially violating the international human rights requirement that "[a]nyone who has been the victim of unlawful arrest or detention shall have an enforceable right to compensation."[262] In such cases, the judges typically found that the arrest or detention was reasonable and lawful – but as the foregoing discussion establishes, officers know or should know from the beginning of an investigation that database information may be inaccurate or can otherwise lead to mistaken conclusions. Courts today therefore should hesitate to regard as reasonable an officer's assumption that personal information in databases is reliable.

Arrests and detentions based on database information alone may even be "arbitrary" in violation of human rights law, especially if the database has known reliability problems or if the officer fails to take account of information contradicting the database, such as a claim of mistaken identity.[263]

262 International Covenant on Civil and Political Rights (ICCPR), adopted December 16, 1966, G.A. Res. 2200A (XXI), 21 U.N. GAOR Supp. (No. 16) at 52, U.N. Doc. A/6316 (1966), 999 U.N.T.S. 171, entered into force March 23, 1976, ratified by the United States on June 8, 1992, art. 9(5).

263 Ibid. art. 9(1)

B. Lookups of victims and bystanders

In several instances that later resulted in federal civil rights lawsuits, court filings suggest that police conducting investigations looked up or received database information about the victim of the alleged crime, or a bystander they had no reason to believe was involved in the offense. Police in the US regularly use force, meaning that instant law enforcement access to database information about people creates a risk that victims and bystanders will have needless interactions with police that can lead to injury or death.

Victims – people in need of help – and bystanders also face a risk of being arrested or detained because of these instant lookups, including when there was no prior reason for an officer to suspect them of any wrongdoing. For victims, this creates a risk that they will not receive the help they need; it also creates a risk that future victims will not call police for assistance. A media report from 2018 and at least one federal lawsuit indicate that people calling for police help could also, in some circumstances, face deportation or removal from the country.[264]

264 *Creedle v. Miami-Dade County et al.*, 349 F. Supp. 3d 1276 (S.D. Fl. 2018); Daniella Silva, "Immigrant faces deportation after calling police for help," NBC News, February 13, 2018, https://www.nbcnews.com/news/us-news/immigrant-faces-deportation-after-calling-police-help-n847801 (accessed October 17, 2024).

Burrell Ramsey-White

In a widely publicized incident during the summer of 2012, two plainclothes Boston police officers responded to a call about a Black man peering into car windows. A later lawsuit claimed that Burrell Ramsey-White, another Black man, happened to be driving in the area but did not match the suspect's description.[265] (The defendants claimed they were unable to see Ramsey-White at this time.)[266] As the defendants acknowledged, instant access to a police database enabled them to look up the license plate number of the car Ramsey-White was driving. When they did, they found that a warrant was linked to the car's owner.[267] Based on the later case records, it appears that Ramsey-White and the car's owner (or at least, the subject of the warrant) were different people.[268]

According to the plaintiff, this instant access to data about a passing car, without any reason to believe the car or driver were involved in a crime, initiated a chain of events that grew from an unnecessary police stop of an innocent person to a deadly use of force. It was agreed that the officers initiated a traffic stop, and that after a conversation (the contents of which were later disputed among the parties to the lawsuit), Ramsey-White began to drive away. The police gave chase and, by the time a supervisor told them to desist, had pursued the driver into a street leading to a dead end; the interaction ended with one of the officers shooting Ramsey-White, who – the plaintiff said – died soon after.[269] Officers have maintained that Ramsey-White brandished a gun at them, while the plaintiff disputed this.[270]

A jury in the civil-rights lawsuit brought by Ramsey-White's mother found in 2019 that the officers were not liable for using excessive force or otherwise violating Ramsey-White's civil rights.[271]

---

265 *Sheffield v. Pieroway et al.*, case no. 1:15-cv-14174 (D. Mass.), 361 F. Supp. 3d 160, Memorandum and Order (doc. 115), February 22, 2019, pp. 1-2.

266 *Sheffield v. Pieroway et al.*, Defendants' Statement of Undisputed Material Facts (doc. 89), September 28, 2018, p. 1.

267 Ibid.

268 See *Sheffield v. Pieroway et al.*, Plaintiff's Response to Defendants' Statement of Material Facts (doc. 98), November 13, 2018, pp. 3-4, and Exhibit 2 (doc. 98-2), p. 16.

269 *Sheffield v. Pieroway et al.*, Plaintiff's Response to Defendants' Statement of Material Facts, pp. 3 et seq. (This response includes the defendants' original statement of material facts.) These statements of material facts do not explicitly confirm that Ramsey-White died, but we are not aware of any dispute between the parties as to whether Ramsey-White died shortly after the shooting. The plaintiff's claim to this effect is provided at *Sheffield v. Pieroway et al.*, First Amended Complaint (doc. 26), April 25, 2016, p. 26.

270 *Sheffield v. Pieroway et al.*, Plaintiff's Response to Defendants' Statement of Material Facts, p. 12.

271 *Sheffield v. Pieroway et al.*, Verdict Form (doc. 185), March 18, 2019; Plaintiff's Motion for a New Trial (doc. 190), April 16, 2019.

J.P.

Officers responding to the domestic violence call received information wrongly indicating that a warrant had been issued for the victim's arrest.

J.P., a multiracial woman, alleged that she had already been arrested and detained twice pursuant to an outstanding warrant issued for another woman when in May 2016, officers responded to a call for assistance during an episode of domestic violence allegedly perpetrated against the five-months-pregnant J.P. (We are using J.P.'s initials due to the case's link with domestic violence.) She has claimed that although the other woman was white and officers had other reasons to know J.P. was not the subject of the warrant, the data was never corrected in their databases. In her claim, J.P. alleged that officers responding to the domestic violence call had therefore received information wrongly indicating that a warrant had been issued for her. The defendants contested J.P.'s version of events and denied any wrongdoing. [272]

The same officers who had been responding to concerns about domestic violence against J.P. allegedly proceeded to arrest her based on the outstanding warrant. J.P.'s subsequent lawsuit resulted in settlements in 2018 and 2019.[273] (We offer a reminder that a settlement is not necessarily an admission of wrongdoing.)

272 Documentation on file with the authors

273 Documentation on file with the authors.

Jayne Cramer

Jayne Cramer (now deceased) claimed in court that she decided to sit on the steps of a house while waiting for a bus in Flint, Michigan, in January 2015. According to Cramer, the house's owner emerged and began an argument that resulted in the owner's boyfriend punching Cramer in the face.[274] When police arrived on the scene, she said, they arrested the person who allegedly committed the assault – but then, Cramer claimed, they decided to look up Cramer, the victim, in one of their databases.[275]

The database appeared to indicate that an arrest warrant had been issued in Florida for someone with the same name, and police proceeded to arrest Cramer – the woman who had called for help.[276] (Court records suggest that the question of whether the Jayne Cramer named in the Florida warrant was the same person as the Jayne Cramer in this case was never resolved.)

Cramer told the court that she was brought to the local jail, strip-searched, and detained for three days.[277] She further claimed that while in detention, she fell in her cell – she was missing toes due to diabetes – and broke her hip.[278]

The court did not reach the stage of making findings of fact, and the disputes in the case largely appear to have centered on Cramer's experiences in jail. However, the court did point out that the record of the database information that had led to Cramer's arrest was minimal: the document summarizing the information about the supposed Florida warrant, the judge said, was "just fifteen lines of text consisting of fewer than 50 'words,' most of which are either abbreviated or single letters," with "no self-authenticating details, such as what database was searched, the query terms used, who searched, whether there were other results, etc." Having scrutinized the document, the judge concluded that it was not clear whether an actual Florida arrest warrant had existed in the first place.[279]

After filing her lawsuit, Cramer passed away in 2018; the case resulted in a settlement with her next of kin in May 2019. [280]

---

274 *Cramer v. Genesee County et al.*, case no. 2:18-cv-10115 (E.D. Mich.), Opinion and Order Granting in Part and Denying in Part Defendant's Motion to Dismiss (doc. 26), June 14, 2018.

275 Ibid.; see also *Cramer v. Genesee County et al.*, Motion to Dismiss (doc. 15), March 29, 2018, p. 13.

276 *Cramer v. Genesee County et al.*, Opinion and Order Granting in Part and Denying in Part Defendant's Motion to Dismiss (doc. 26), pp. 1-2; see also Motion to Dismiss (doc. 15), pp. 13-14.

277 *Cramer v. Genesee County et al.*, Defendant Beagle's Answer to Plaintiff's First Amended Complaint (doc. 6), January 24, 2018, p. 6; Triplett v. Genesee County et al., case 2:18-cv-10115 (E.D. Mich.), Defendant Beagle's Motion for Summary Judgment (doc. 52), April 20, 2019, p. 2; *Cramer v. Genesee County et al.*, Opinion and Order (doc. 26), p. 2.

278 *Triplett v. Genesee County et al.*, Defendants' Motion for Summary Judgment (doc. 49), April 17, 2019, pp. 12-16.

279 *Cramer v. Genesee County et al.*, Opinion and Order Granting in Part and Denying in Part Defendant's Motion to Dismiss (doc. 26), p. 6,

280 Ibid. at p. 6; *Triplett v. Genesee County et al.*, Order of Dismissal (doc. 54), June 13, 2019.

Phillip Armijo

In March 2016, Phillip Armijo called the police in Santa Fe, New Mexico, during an argument with his sister, who he alleged was breaking windows.[281] Although the record does not disclose any reason for the authorities to believe Armijo had done anything wrong, a dispatcher responding to the call used a law enforcement database to look up both Armijo and his sister.[282] As officers later realized, the database results stated that a warrant had been issued for John Armijo, Phillip's brother, for driving under the influence of intoxicants – and it claimed that "Phillip M. Armijo was an alias for John K. Armijo."[283]

Phillip Armijo, who had been calling for help, therefore faced all the risks associated with US police officers' use of large law enforcement databases -- including the risk of an arrest based on mistaken identity. In his case, that risk came to pass: he was arrested at the scene and detained before a court ordered his release due to mistaken identity.[284] His later lawsuit against local officials ended in a settlement in 2018.[285]

281 *Armijo v. Santa Fe County et al.*, case no. 1:17-cv-00574 (D. N.M.), City Defendants' Motion for Summary Judgment (doc. 32), November 22, 2017, p. 3; Plaintiff's Cross Motion for Summary Judgment (doc. 40), January 8, 2018, p. 2.

282 *Armijo v. Santa Fe County et al.*, Plaintiff's Cross Motion for Summary Judgment (doc. 40), pp. 3-4; City Defendants' Motion for Summary Judgment (doc. 32), p. 3; Memorandum Opinion and Order (doc. 53), June 25, 2018, pp. 4-6.

283 *Armijo v. Santa Fe County et al.*, Motion for Summary Judgment (doc. 32), pp. 3-5.

284 *Armijo v. Santa Fe County et al.*, Memorandum Opinion and Order (doc. 53), pp. 5, 8-9.

285 *Armijo v. Santa Fe County et al.*, Stipulation of Dismissal (doc. 62), October 10, 2018.

Johnnie Rochell, Jr.

In another 2016 episode, a plainclothes Arkansas police detective was surveilling a house from an unmarked vehicle when a neighbor, Johnnie Rochell, Jr., became concerned about his presence.[286] When the officer declined to lower his window and speak to Rochell, Rochell (who was unaware that the man was a member of the police) returned to his home and re-emerged with an AR-15 rifle slung across his back.[287] Although the records we examined do not explain why Rochell reacted with such great concern, the district court did not appear to take issue with this decision, and we infer from the circumstances that Rochell had a license to own and carry the firearm.[288]

During the tense exchange that ensued, the detective revealed that he was a police officer, and Rochelle removed his weapon and stepped away from it. The detective then forced Rochell at gunpoint – at virtually point-blank range, according to the officer's later account – to lie on the ground and handcuffed him.[289]

Another officer who had arrived at the scene asked a dispatcher to search a state law enforcement database and NCIC for people linked to Rochell's address who had past convictions (which can render gun possession illegal) or outstanding warrants,[290] although the records we examined do not reveal any reason for the officers to have believed, at the time, that Rochell or anyone else in his home was – or ever had been – involved in criminal activity. (In the United States, where many states have relaxed laws on gun ownership, merely having a powerful rifle in the home is not necessarily an indication that someone is involved in crime).

For reasons that are not clear, the databases returned results including information about both Rochell, a Black man with no felony convictions, and a white man with the same birthdate (but a different name) who did have such convictions. As a result of the database hits and, it appears, mistaken searches based on those results, the dispatcher reported to the police at the scene that Rochell, not the white man, had felony convictions.[291] As a result, Rochell was arrested on the grounds that it was unlawful for him, as a purported felon, to possess a firearm.[292] Rochell was detained overnight before posting bond.[293]

---

286 *Rochell v. City of Springdale, Arkansas et al.* (later titled Rochell v. Ross), case no. 5:16-cv-05093 (W.D. Ark.), Memorandum Opinion and Order (doc. 69), October 25, 2017, pp. 1-2; cf. *Rochell v. City of Springdale, Arkansas et al.*, Defendants' Statement of Undisputed Material Facts (doc. 53), August 2, 2017, p. 4.

287 Memorandum Opinion and Order (doc. 69), p. 2; cf. Defendants' Statement of Undisputed Material Facts (doc. 53), pp. 5-6.

288 E.g., law enforcement relinquished the gun to Rochell after the discovery of the mistaken identity error described in the paragraphs below. Defendants' Statement of Undisputed Material Facts, p. 11.

289 Memorandum Opinion and Order, pp. 3-6; cf. Defendants' Statement of Undisputed Material Facts, pp. 6-7.

290 Memorandum Opinion and Order, pp. 6-8; cf. Defendants' Statement of Undisputed Material Facts, pp. 7-9.

291 Ibid.

292 Memorandum Opinion and Order, pp. 8; cf. Defendants' Statement of Undisputed Material Facts, p. 9.

293 Memorandum Opinion and Order, pp. 8-9.

A few days later, one of the arresting officers became concerned that he may have made a mistaken arrest, and soon determined that he had done so.[294] However, in the court's words: "Instead of putting this case of mistaken identity behind him, the next thing [the detective] did was confer with his supervisor to figure out how to charge Mr. Rochell with something else" (emphasis in the original).[295] (We invite the reader to recall that at this stage, the court was construing the facts in the light most favorable to Rochell.) After consulting a law book, the police sought a charge against Rochell for misdemeanor disorderly conduct, and Rochell was later convicted of that offense.[296]

This meant that an at least arguably unnecessary database search for past convictions or outstanding warrants had drawn Rochell into a web of the consequences that can result from encounters with US authorities, such as mistaken identity or retaliation.

In 2019, The Eight Circuit Court of Appeals affirmed a decision by the district judge that the defendant officer could not claim qualified or other immunity, as his choice to point a gun at Rochell's head while Rochell was on the ground and posed no threat violated a constitutional right that was clearly established.[297] In 2021, after a trial, Rochell's civil rights lawsuit resulted in a jury verdict that the arresting officer had used excessive force and that his conduct had involved "reckless or callous indifference to Mr. Rochell's Fourth Amendment rights." The jury awarded $7,000 in punitive damages.[298]

294 Memorandum Opinion and Order, pp. 9-10; cf. Defendants' Statement of Undisputed Material Facts, pp. 9-10.

295 Memorandum Opinion and Order, p. 11.

296 Ibid.

297 Rochell v. City of Springdale et al., 768 Fed. Appx. 588 (8th Cir.), April 25, 2019.

298 Rochell v. Ross, case no. 5:16-cv-5093, Jury Verdict (doc. 183), September 22, 2021.

What went wrong

These cases point to the ease with which officers, dispatchers or other law enforcement personnel may search for personal data about people whom they otherwise have no reason to suspect of wrongdoing – even when those people are seeking help or are mere bystanders.

Such suspicionless lookups can needlessly create or prolong encounters between individuals and police, with the potential for mistakes, the use of force, and other negative consequences. They also raise concerns about whether police or dispatchers are treating all members of their local communities as potentially suspect by default.

We are particularly concerned about the human rights harms that may arise if crime victims are deterred from calling for help because they are afraid they will be mistakenly or needlessly arrested.

C. Allegedly racist enforcement

i. Driving while Black, existing while Romani: suspicionless lookups of people of color and/or their vehicles

For decades, activists and scholars in the US have documented disproportionate police stops of drivers of color — a phenomenon racial justice advocates often decry as stops simply for "driving while Black."[299]

Federal civil rights lawsuits we examined suggest to us that "driving while Black" (or belonging to a racial minority group more broadly), and police access to large databases in their patrol cars, can be a dangerous and even deadly combination for the driver and passengers. While we cannot prove that the police or other government behaviors in these cases were motivated by racism, we see these cases as forming a disturbing pattern that highlights a potential danger.

Even the humiliation of a brief stop and handcuffing, as occurred to Black driver and lawyer Linda Perkins-Moore in late 2019 following an officer's database search of her license plate for no reason other than that she was on a public road, can be considerably affecting for some people. The court dismissed Perkins-Moore's case on the grounds that the officers had not acted illegally: in the United States, it is lawful for police to look up someone's license plate for no reason[300], and plaintiffs face an almost insurmountable hurdle in arguing that officers had racist intent, as this is often difficult or impossible to prove.

---

299 See, e.g., David A. Harris, "Driving While Black: Racial Profiling on Our Nation's Highways," American Civil Liberties Union, June 1999, https://www.aclu.org/report/driving-while-black-racial-profiling-our-nations-highways (accessed October 17, 2024); Erik Ortiz, "Inside 100 million police traffic stops: New evidence of racial bias," NBC News, March 13, 2019, https://www.nbcnews.com/news/us-news/inside-100-million-police-traffic-stops-new-evidence-racial-bias-n980556 (accessed October 17, 2024).

300 *Perkins-Moore v. City of Detroit et al.*, case no. 2:21-cv-10929 (E.D. Mich.), Opinion & Order Granting Defendants' Motion for Summary Judgment (doc. 91), June 15, 2023, pp. 5, 11-12; Judgment (doc. 92), June 15, 2023. – case not on file, unable to verify in full

Clarence Jamison

At the same time, a database search that returns no results, or only "clean" ones, may not be enough to prevent a racist traffic stop or other racist police action – a point illustrated by a livid judgment by the federal district court for the Southern District of Mississippi in Jamison v. McClendon in August 2020. The case arose in 2013 after an officer ran a database search on driver Clarence Jamison, who is Black, and then – despite the clean results – detained Jamison for nearly two hours.[301] We reiterate that it is impossible to know what is in officers' minds. However, the federal judge in this case was clearly of the opinion that Jamison's detention was connected with his race: in a litany of allusions to some of the US police harms against Black people that were part of the public conversation after the murder of George Floyd (see above), the judge wrote:

"Clarence Jamison wasn't jaywalking.

He wasn't outside playing with a toy gun.

He didn't look like a 'suspicious person.'

He wasn't suspected of 'selling loose, untaxed cigarettes.'

He wasn't suspected of passing a counterfeit $20 bill.

He didn't look like anyone suspected of a crime.

He wasn't mentally ill and in need of help.

He wasn't assisting an autistic patient who had wandered away from a group home.

He wasn't walking home from an after-school job.

He wasn't walking back from a restaurant.

He wasn't hanging out on a college campus.

He wasn't standing outside of his apartment.

He wasn't inside his apartment eating ice cream.

He wasn't sleeping in his bed.

301 *Jamison v. McClendon*, case no. 3:16-cv-00595 (S.D. Miss.), Order Granting Qualified Immunity (doc. 72), August 4, 2020, pp. 4, 6-7.

He wasn't sleeping in his car.

He didn't make an 'improper lane change.'

He didn't have a broken tail light.

He wasn't driving over the speed limit.

He wasn't driving under the speed limit.

No, Clarence Jamison was a Black man driving a Mercedes convertible.

As he made his way home to South Carolina from a vacation in Arizona, Jamison was pulled over and subjected to one hundred and ten minutes of an armed police officer badgering him, pressuring him, lying to him, and then searching his car top-to-bottom for drugs.

Nothing was found. Jamison isn't a drug courier. He's a welder.

Unsatisfied, the officer then brought out a canine to sniff the car. The dog found nothing. So nearly two hours after it started, the officer left Jamison by the side of the road to put his car back together.

Thankfully, Jamison left the stop with his life. Too many others have not." [302]

The judge found that the officer's search of Jamison's car had violated the Fourth Amendment, based partly on a conclusion that Jamison, a Black man driving in a region with a long history of fatal anti-Black violence, had not consented freely to the search. Yet, the judge found that he had no choice but to apply the law of qualified immunity as articulated by the US Supreme Court and dismiss the case – even while echoing an appellate court in pleading, "This has to stop."[303]

The case appears to have ended with a settlement agreement on the same day the judge's opinion was released in 2020.[304]

302 Ibid. at pp. 1-5.

303 Ibid. at pp. 6, 46-56.

304 *Jamison v. McClendon*, case no. 3:16-cv-00595, Stipulation of Dismissal (doc. 73), August 4, 2020.

Robert Tolan

In a case that had reached the US Supreme Court several years before the officer in Mississippi stopped Clarence Jamison, a police officer patrolling a suburb of Houston, Texas in 2008 saw a vehicle make a rapid turn and park in front of a home.[305] (We recall here, as the Court also did, that it was presenting the allegations and/or evidence in the record in the light most favorable to Tolan.) In the version of the facts recited by the Court, Robert Tolan, a Black man, and his cousin emerged from the car.[306] The officer then tried to enter the car's license plate number into a database, but entered an incorrect number.[307] The parties later disagreed about whether the rapid turn the officer said he had observed provided reasonable grounds for suspecting that any criminal offense was occurring.[308]

The police database indicated that the (incorrect) plate number the officer had entered belonged to a stolen car, and the computer automatically broadcast a message to other police about the suspected crime. When the officer approached the men and drew his gun, Tolan explained that the car was his — and his parents soon emerged from the house to confirm this claim. Nevertheless, the officer ordered Tolan and his cousin onto the ground, and a second officer who arrived on the scene shortly afterward shot Tolan in the chest during an ensuing disagreement.[309]

Tolan survived the shooting, and in 2014, the Supreme Court found unanimously that a lower court had been wrong to grant summary judgment in favor of one of the officers regarding the question of whether the shooting was lawful.[310] The case ended in a settlement in 2015.[311]

---

305 *Tolan v. Cotton*, 572 U.S. 650, 651 (2014).

306 Ibid.; regarding Tolan's race, see James C. McKinley Jr., "Texas Officer Is Acquitted in Shooting," *New York Times*, May 11, 2010, https://www.nytimes.com/2010/05/12/us/12houston.html (accessed October 17, 2024).

307 *Tolan v. Cotton*, 572 U.S. 650, 651-652 (2014).

308 *Tolan et al. v. Cotton et al.*, case no. 4:09-cv-1324 (S.D. Tex.), Complaint (doc. 1), May 1, 2009, para. 75 (maintaining that there were no reasonable grounds for an officer to suspect that an offense had occurred); Defendants' Motion for Summary Judgment (doc. 67), January 1, 2011, para. 48 (arguing that "the manner in which the driver of the [sport utility vehicle] executed a turn raised an articulable suspicion in [the officer's] mind that the driver may have not planned to turn onto a dead end street until the last moment").

309 *Tolan v. Cotton*, 572 U.S. 650, 652-654 (2014).

310 *Tolan v. Cotton*, 572 U.S. 650 (2014).

311 Cameron Langford, "Police Shooting Trial Ends With Surprise Settlement," Courthouse News Service, September 15, 2015, https://www.courthousenews.com/police-shooting-trial-ends-with-surprise-settlement/ (accessed October 17, 2024).

L.D.

A police search for data about L.D. as she was driving in 2012 also ended badly.[312] As L.D., a 40-year-old Black woman, drove through a town in the western US one winter night, an officer decided to look up her license plate number in a police database and found information suggesting that a warrant had been issued for L.D.'s arrest; as the appeals court later explained, the charge was driving with a license that had been suspended—a misdemeanor.[313] Police filings in the lawsuit that ultimately resulted from this episode do not disclose any reason for the database search.[314]

The officer who had looked up L.D.'s plate number proceeded to pull her over and was soon joined by three other officers.[315] The incident report and court records indicate that L.D. expressed frustration to the officer, who told L.D. that she was under arrest and ordered her to get out of the car. Two more police cars and several other officers had arrived at the scene and surrounded L.D.s vehicle. L.D. did not immediately get out of the car.

At some point thereafter, an officer at the scene smashed L.D.'s window with a baton. The five-foot-two-inch, 115-pound L.D., whom a doctor later described as having "significant mental health issues as well as chronic pain and disability" predating the incident, was handcuffed and placed on the ground, and after being taken to the hospital for an examination, she was detained in jail.[316] Her federal lawsuit resulted in a settlement after an appellate court found that her case—viewed in the light most favorable to her—was able to overcome two of the officers' qualified immunity, at least at the pre-trial stage.[317]

312 Demographic data obtained from incident report on file with the authors. While the records from L.D.'s lawsuit are public and include her full name, and while her name has also appeared in the media, we have chosen to use initials for this plaintiff due to the inclusion of information pertaining to her health.

313 Documentation on file with the authors.

314 Documentation on file with the authors.

315 Documentation on file with the authors.

316 Documentation on file with the authors.

317 Documentation on file with the authors.

Christopher Bey

"I'm thinking we're in Russia or something.... The Court would find that there was absolutely no reason in the world to stop these people."

According to claims made in a Michigan case, on a winter night in 2013, Christopher Bey and two friends – all of them young Black men – drove to a series of large 24-hour stores to shop for a space heater.[318]

Unbeknownst to the three men, a police officer started following them and – according to the police defendants' later account – asked a dispatcher to search Michigan's LEIN database for the temporary license number displayed on the men's car.[319] When the dispatcher allegedly stated that the number did not appear in LEIN, the officers continued their surveillance of the three friends, even though they later stated that LEIN sometimes did not contain records of valid temporary numbers – and even though there was no other reason to suspect Bey or his friends of any wrongdoing. (The court cited the officers' depositions in presenting this version of the factual claims.)[320] The district court later remarked pointedly that "a reasonable fact finder could determine that the purported 'no report' result [in LEIN] was nothing more than a made up reason for a stop," although the police insisted that they had not invented the LEIN search.[321]

According to Bey's version of events (regarding which the court also cited the officers' later depositions in places), multiple officers followed the men on their shopping journey, observing them as they browsed various items and made purchases, and the police eventually surrounded the men in a parking lot. After an officer ordered Bey out of the vehicle, Bey told the officer he had a weapon for which he had a license. Bey gave the officer his weapon and the license, but when the officer checked the license, he found that it was expired. The officer then arrested Bey for carrying a concealed weapon unlawfully, a felony.[322]

---

318 *Bey v. Falk et al.*, case no. 2:14-cv-13743 (E.D. Mich.), Opinion (doc. 53), March 29, 2017, pp. 2-3, recounting allegations made in Plaintiff's Response in Opposition to the City of Livonia Defendants' Motion for Summary Judgment (doc. 46), July 25, 2016, p. 9.

319 *Bey v. Falk et al.*, Opinion (doc. 53), pp. 5, 17; cf. *Bey v. Falk et al.*, Livonia Defendants' Reply Brief (doc. 49), August 15, 2016, p. 3.

320 Opinion (doc. 53), pp. 5, 17.

321 Opinion (doc. 53), p. 17; Reply Brief (doc. 49), p. 3.

322 Opinion (doc. 53), pp. 3-10.

During the criminal prosecution of Bey in state court, the judge in those proceedings suppressed evidence about the gun, finding that there was no basis for the stop that led officers to seize it. During a hearing, the state court judge said: "I'm thinking we're in Russia or something. I'm not sure what's going on here.... This is a no-brainer.... The Court would find that there was absolutely no reason in the world to stop these people."[323]

These criminal charges against Bey were then dismissed with prejudice (meaning that prosecutors could not try to bring those charges again), and Bey brought a suit in federal court for violations of his constitutional rights.[324] The federal judge allowed some of his claims to proceed (while rejecting others) in 2017; the Sixth Circuit Court of Appeals then found in late 2019 that most of the officers who had been involved in the stop were entitled to qualified immunity.[325] The remainder of the case appears to have ended in a settlement in 2020, although this is not explicit in the record.[326]

The circumstances of the Bey case point to the possibility that officers in the US could use database searches after the fact to try to justify an arrest they have already made, regardless of whether that is in fact what happened in this instance. (We recall that in Bey, the relevant officer denied this.)

323 Ibid., pp. 10-11.

324 Ibid. p. 11; *Bey v. Falk et al.*, Plaintiff's First Amended Complaint and Jury Demand (doc. 12), April 20, 2015, p. 2.

325 Opinion (doc. 53), pp. 40-41; Bey v. Falk et al., case no. 2:14-cv-13743 (6th Cir.), Opinion (doc. 70), December 31, 2019, p. 8 of PDF.

326 See *Bey v. Charter Township of Canton, Michigan et al.*, case no. 2:14-cv-13743 (E.D. Mich.), Stipulated Order of Dismissal (doc. 82), September 30, 2020. We infer from this stipulated dismissal, following on from the Sixth Circuit opinion allowing Bey's suit to proceed in part, that a settlement likely took place; however, we cannot be sure based on the record. We offer a reminder that a settlement is not an admission of wrongdoing.

Bianca Johnson and Delmar Canada

Database searches by a police officer looking up the license plates of people visiting a budget motel and convenience store in Charlottesville, Virginia on a spring afternoon in 2014 led to a claim by a Black couple of racially targeted policing.

According to a court opinion refusing to grant the police officers' motion to dismiss the case before trial, an officer parked his car in the hotel parking lot with a view of a nearby 7-Eleven store on an April day. The officer claimed his goal that day was to use traffic laws to initiate stops of cars and carry out anti-drug enforcement in an area where he said there had been narcotics activity.[327] While doing so, he searched a Virginia law enforcement database for the license plate numbers of cars that were present in the 7-Eleven lot, without any apparent basis for believing that the people who owned the cars had been engaged in any criminal activity.[328]

The database results indicated that a license plate affixed to a BMW belonged to Bianca Johnson, and the officer later claimed that upon viewing the name, he was reminded of a call to the police about some situation involving Johnson and her male partner.[329] The officer then – again without any apparent suspicion that Johnson was engaged in wrongdoing – "searched either the Pistol or LinX police databases, to inquire into persons associated with Johnson" and "found that Delmar Canada was an associate of Johnson's.... By clicking on a hyperlink associated with Canada, [the officer] was able to pull up a picture of Canada."[330] (Law Enforcement Information Exchange, or "LInX," is a data analysis platform that our research suggested was offered to police by a private company, at least as of 2019, although it may now be government-run; we have been unable to confirm the nature of "Pistol.")[331] According to the police, one of the databases suggested that Canada's driver's license had been suspended.[332]

---

327 *Johnson et al. v. Holmes et al.*, case no. 3:16-cv-00016 (W.D. Va.), Memorandum Opinion on Defendant's Motion for Summary Judgment (doc. 57), October 19, 2017, pp. 1-2.

328 Ibid.; *Johnson et al. v. Holmes et al.*, Defendants' Memorandum in Support of Motion for Summary Judgment (doc. 46), August 28, 2017, p. 2.

329 Ibid.

330 Ibid.

331 Northrop Grumman, "Law Enforcement Information Exchange (LInX)," https://www.northropgrumman.com/Capabilities/PublicSafety/Pages/LawEnforcementInformationExchange.aspx (accessed August 23, 2019 and archived at https://web.archive.org/web/20190711034046/https://www.northropgrumman.com/Capabilities/PublicSafety/Pages/LawEnforcementInformationExchange.aspx).

332 *Johnson et al. v. Holmes et al.*, Defendants' Memorandum in Support of Motion for Summary Judgment (doc. 46), p. 3. See also, Memorandum Opinion on Defendant's Motion for Summary Judgment (doc. 57), October 19, 2017, pp. 2-3, implicitly presenting this claim as uncontested.

After viewing Canada's picture, the officer noticed that a man who resembled the image was entering the BMW.[333] After Canada exited the 7-Eleven and turned onto another street, the officer initiated a traffic stop and issued Canada a summons for driving with a suspended license.[334] In the meantime, Johnson had arrived and asked for the officer's badge number.[335] The following day, in a first for the officer and an apparent first for his department, the officer applied for a warrant to search Canada's home for evidence that he had previously received paperwork from the state's Department of Motor Vehicles related to the license suspension. A few days later, the officer carried out a search of Canada's house late at night.[336]

In 2014, Johnson and Canada filed a complaint of biased policing with the police department, and in 2016, they filed a civil rights lawsuit claiming the officer had targeted them because they were Black. [337]

An internal affairs investigation into their complaint did not ascribe any racially motivated wrongdoing to the officer.[338] In the federal civil rights suit, a judge initially allowed the plaintiffs' equal protection claims (which concerned the house search) to move forward on the grounds that a jury could have reasonably inferred that the officer was motivated by bias. For example, the judge noted that "a reasonable jury could find that the officer's belief that he would find narcotics in the plaintiffs' residence was grounded in the unwarranted and race-based assumption that African-Americans driving expensive cars are likely to be involved in drug trafficking."[339] At the end of the case in 2018, a different judge granted judgment in favor of the defendants, finding that because the plaintiffs had not presented any evidence that the officer had behaved differently towards people of other races in similar circumstances, no equal protection violation had been established; in 2019, the Fourth Circuit Court of Appeals disagreed, ruling that this framing of the issue had been too narrow.[340] The case appears to have resulted in a settlement in 2023.[341]

---

333 *Johnson et al. v. Holmes et al.*, Defendants' Memorandum in Support of Motion for Summary Judgment (doc. 46), pp. 2-3.

334 *Johnson et al. v. Holmes et al.*, Memorandum Opinion on Defendant's Motion for Summary Judgment (doc. 57), October 19, 2017, pp. 2-3.

335 Ibid. at p. 3; it appears that the exchange was recorded on video.

336 *Johnson et al. v. Holmes et al.*, Defendants' Memorandum in Support of Motion for Summary Judgment, Exhibit 1 (doc. 46-1), pp. 1-2; Memorandum Opinion (doc. 57), October 19, 2017, pp. 4-5.

337 *Johnson et al. v. Holmes et al.*, Defendants' Memorandum in Support of Motion for Summary Judgment, Exhibit 1 (doc. 46-1); First Amended Complaint and Jury Demand (doc. 20), April 8, 2016.

338 *Johnson et al. v. Holmes et al.*, Defendants' Memorandum in Support of Motion for Summary Judgment, Exhibit 1 (doc. 46-1), pp. 6-7.

339 *Johnson et al. v. Holmes et al.*, Memorandum Opinion (doc. 57), pp. 12-14.

340 *Johnson et al. v. Holmes et al.*, Memorandum Opinion and Order (doc. 91), March 22, 2018, p. 1; *Johnson et al. v. Holmes et al.*, case no. 18-1454 (6th Cir.), Opinion, (doc. 105) August 27, 2019, p. 4.

341 See *Johnson et al. v. Holmes et al.*, Findings of Fact and Conclusions of Law (doc. 280), August 29, 2023 (addressing a dispute about the settlement).

Clark Demetro

In what we see as a particularly stark case, an anti-fraud non-profit organization that says it is comprised of "law enforcement and associated professionals in the United States, Canada, Germany, and the United Kingdom" maintained a database as part of a website that (at the time of the relevant events) included what a federal judge described as "appalling" language about people with Romani heritage. The site, the judge stated, had "a history of publishing articles that include[d] racially charged generalizations about persons of Romani descent," and the plaintiffs alleged that the organization had labeled some people in its database with the marker "G" for "Gypsy"—a term for Romani people that some regard as a slur.[342] The plaintiffs also alleged that website's slogan at the time of the relevant events was "Ignorance is the Gypsies' weapon against the outside world."[343] (As of the time of our research, the site appeared to have removed any anti-Romani language and focused on fraud against elderly persons.)

As a policing entity that was not formally part of any government, the organization—the judge said—"occupied a sort of queasy middle status between official and unofficial."[344] This phenomenon of law enforcement databases or software systems that are maintained by private businesses or non-profits, but used exclusively by (or mainly intended for) police, is one that human rights groups and scholars have described in other US contexts.[345] Although an examination of this phenomenon is beyond the scope of this report, it has been creating significant problems in the US for people charged with crimes and those seeking to hold police to account for alleged abuses.[346]

In this case, Clark Demetro—a New Jersey man of Romani descent who had operated a home renovation business—said he discovered that he was listed in the database with the label "G/M" (Gypsy/male), alongside a description of past arrests, convictions, and other ostensible encounters with the criminal justice system.[347] After a 2014 dispute between Demetro and a customer, a police officer trying to locate Demetro had uploaded the man's personal information to the anti-fraud database (although the officer did not use racial indicators when making this entry).[348] Demetro, who pleaded guilty to an offence and was

342 June 25, 2019, pp. 2-7.

343 Ibid., pp. 5, 36-37.

344 Ibid., p. 2.

345 See, e.g., Human Rights Watch, "Letter to US Department of Justice About Child Protection System Software," February 1, 2019, https://www.hrw.org/news/2019/04/03/letter-us-department-justice-about-child-protection-system-software.

346 See, eg. Justin Yu, "The Slippery Slope of Big Data in Policing", *Harvard International Review*, May 27, 2021, https://hir.harvard.edu/big-data-in-policing/ (accessed October 17, 2024); Sam Biddle, "LexisNexis to Provide Giant Database of Personal Information to ICE", *The Intercept*, April 2, 2021, https://theintercept.com/2021/04/02/ice-database-surveillance-lexisnexis/ (accessed October 17, 2024).

347 *Demetro et al. v. National Association of Bunco Investigators et al.*, Opinion (doc. 100), June 25, 2019, pp. 4, 7.

348 Ibid. pp. 9 et seq.

sentenced to probation, discovered this and other entries about him in the database and brought a suit on defamation, equal protection and other grounds against the non-profit organization, the officer who had uploaded his information following the 2014 incident, and the relevant city authority. In 2019, the federal district court dismissed the defamation claim and a claim regarding discrimination in public places, but allowed an equal protection claim on the basis of alleged racial profiling by law enforcement to proceed.[349] In doing so, the judge found that there was enough evidence to justify a further inquiry into whether law enforcement had engaged in discrimination against Demetro because of his Romani heritage, as well as sufficient reason to avoid applying the qualified immunity doctrine for the time being.[350]

The case ended in a settlement in 2021.[351] As a reminder, a settlement is not necessarily an admission of wrongdoing.

349 Ibid. at pp. 23 et seq.

350 Ibid. at pp. 35-40.

351 *Demetro et al. v. National Association of Bunco Investigators et al.*, Order of Dismissal (doc. 127), May 10, 2021.

What went wrong

Taken together, these cases provide evidence that US officers can and sometimes do use their access to large collections of personal data to carry out suspicionless searches for information about people who simply happen to cross their paths – including, in many cases, people of color.

The cases prompt concerns that in practice, there is little to prevent officers in the US from carrying out racially based fishing expeditions using large databases – and that such searches can lead to arrests or initiate chains of events that end in officers' use of force (although this is not always what happens). There is also a clear risk that officers will act on information to which they have access even if there is no compelling need for them to be able to see that information.

These large databases implicitly treat everyone as a potential suspect – but in the United States, people from Black, Latin American and other minority racial backgrounds already face other layers of suspicion due to racism. In our view, this means that while the "collect-it-all" mentality of those who create police databases impacts everyone, that seeming equality likely does not survive encounters with the reality of actual, everyday policing in America.

ii. The "worst of the worst"? Databases and alleged race-based policing in the Albuquerque "Surge" operation

A 2016 ATF operation in Albuquerque, New Mexico known as the "Surge" offers a cautionary tale about the ways warrantless police database use could facilitate discriminatory law enforcement.[352]

During the operation, the ATF sent confidential informants to a largely minority area of the city with general instructions to develop leads about who might be engaging in crime and no training about implicit bias. These informants collected phone numbers from the people they met, used a database (potentially from the private sector) to connect phone numbers to names without any subpoenas or other legal process, and then searched NCIC to find out if the person had a criminal record.[353] If they did, the ATF directed the confidential informant to continue pursuing the person as a target for investigation.[354]

In sum, people became targets of this investigation because someone on the street or in a shop gave a confidential informant a telephone number, a database linked the telephone number with the person's name, and the person happened to be listed in another database as having a criminal record.

The end result of the operation was a set of more than 100 arrests in which about 84 percent of the defendants were Black or of Latin American descent – in a city where these groups made up only about 50 percent of the population as a whole. While white people comprised about 42 percent of the city's residents, only 14.5 percent of the defendants prosecuted during the "Surge" were white.[355]

Instant, warrantless access to NCIC and the other database were not the sole causes of the operation's racially disproportionate outcome – but were crucial links in the chain of investigative decisions that produced it.

352 Testimony in 2017 by a special agent of the Bureau of Alcohol, Tobacco, Firearms and Explosives confirms that the operation had been known as the "Surge." *United States v. Laneham*, case no. 1:16-cr-2930 (D. N.M.), Transcript of Motion Proceedings (doc. 132), October 4, 2017, pp. 4-5. At the time, the term would have recalled certain US military operations in Iraq.

353 Ibid. at pp. 4-18.

354 See, e.g., ibid., pp. 18-34.

355 Jeff Proctor, "Feds' sting ensnared many ABQ blacks, not 'worst of the worst'", *New Mexico In Depth*, May 7, 2017, https://nmindepth.com/2017/feds-sting-ensnared-many-abq-blacks-not-worst-of-the-worst/ (accessed October 17, 2024).

As the ATF special agent who led the investigation later testified, the "Surge" was an "Enhanced Enforcement Initiative" by the agency; a 2015 ATF fact sheet describes such initiatives as part of a concerted effort to engage in "intelligence-driven" law enforcement.[356] According to the ATF, enhanced enforcement initiatives focused on "[c]ities or regions identified ... as experiencing a disproportionate firearms-related violent crime problem or a sharp escalation in such crime."[357] The special agent testified in other cases that after selecting Albuquerque for an enhanced enforcement initiative, the agency chose to focus on "the southeast quadrant" of the city in consultation with other authorities – although the agent also acknowledged under questioning that the ATF did not use any crime statistics or reports when choosing this area, instead relying on local law enforcement officers' impressions.[358] Local media reporting has characterized the "Surge" effort as focusing on "a largely minority swath" of the city.[359]

To carry out the "Surge," the ATF sent five confidential informants to the area it called the southeast quadrant. Three of these secret informants were Black, and two were of Latin American descent.[360] By contrast, the population of Albuquerque was 42 percent white, three percent Black, and 47 percent of Latin American descent.[361] Neither the ATF agent in charge of the operation nor the confidential informants had received any training on avoiding implicit racial bias.[362]

The informants also were not directed to any specific locations to investigate potential crime, or given training about which people to approach as likely suspects. As the lead agent testified, "They weren't told anything other than, 'When you meet people, let us know so we can find out what the guy's background is.'"[363]

On the stand, the agent explained how the investigations during the "Surge" proceeded: a confidential informant would "meet individuals, [and] he would ask them, 'Are you in the game? Do you gangbang? Do you sell drugs? Do you sell guns? Do you do robberies?'" The informant "would then try to get the person's phone number" and pass the number on to the ATF agent.[364]

---

356 *United States v. Laneham*, Transcript of Motion Proceedings (doc. 132), October 4, 2017, p. 5; Bureau of Alcohol, Tobacco, Firearms and Explosives, "Fact Sheet: ATF Frontline," February 2015, https://www.atf.gov/file/10941/download (accessed October 17, 2024).

357 "Fact Sheet: ATF Frontline," February 2015.

358 *United States v. Casanova*, case no. 1:16-cr-2917 (D. N.M.), Transcript of Motion Hearing (doc. 51), April 3, 2017, p. 33; *United States v. Coleman and Jackson*, case no. 1:16-cr-02362 (D. N.M.), Transcript of Proceedings (doc. 62), November 18, 2017, pp. 74-75.

359 Jeff Proctor, "Feds' sting ensnared many ABQ blacks, not 'worst of the worst'" May 7, 2017; *United States v. Coleman and Jackson*, Transcript of Proceedings (doc. 62), November 18, 2017, pp. 74-75.

360 *United States v. Laneham*, Transcript of Motion Proceedings (doc. 132), October 4, 2017, pp. 37-38; *United States v. Casanova*, Transcript of Motion Hearing (doc. 51), April 3, 2017, p. 40.

361 Jeff Proctor, "Feds' sting ensnared many ABQ blacks, not 'worst of the worst'" May 7, 2017.

362 *United States v. Casanova*, Order Granting Discovery (doc. 57), June 12, 2017, pp. 3-4.

363 *United States v. Coleman and Jackson*, Transcript of Proceedings (doc. 62), November 18, 2017, pp. 88-96

364 *United States v. Casanova*, Transcript of Motion Hearing (doc. 51), April 5, 2017, pp. 64-65.

The phone number was important because the ATF agents running the operation could enter it into a database to find the name of its ostensible subscriber or user – which the ATF hoped would allow it to identify the person the informant had met. (It appears that the Albuquerque residents the informants encountered were more likely to share their phone numbers – or other people's – than their names during initial conversations.) Available information suggests that NCIC does not (or, at the time, did not) contain phone numbers, and the government never publicly disclosed what database it used to link phone numbers to names.

During the pretrial process, federal public defenders asked a court to order the disclosure of any reports from the private-sector database TLOxp that were used during the "Surge" investigations, although they did not discuss their reasons for suspecting that the ATF had used this system.[365] In response, the government stated that "this information does not exist."[366] Federal procurement records indicate that the ATF had purchased access to TLOxp since at least 2014, but whether agents used this database as part of the "Surge" investigations – perhaps prior to using NCIC – remains unknown, and there is nothing in the public record to indicate this.

In court, the lead ATF agent explained how his agency chose its investigative targets after linking phone numbers to names: agents searched for the names in NCIC to see if the individuals had criminal records. None of these database searches required any pre-existing reason to believe the person connected to the phone number was currently involved in wrongdoing.[367]

"A lot of people will try to portray themselves as a bad guy so they look cool on the street," the agent told the court, "but once the CI [confidential informant] gets the phone number, if the individual has no criminal history, and they are saying they sell guns and drugs and do robberies, the CI's are instructed, 'Don't talk to that guy anymore.'"[368] However, when agents identify someone (including by first getting their phone number), "and we see he has three or four felony convictions, a sex assault arrest, and he says that he can do guns and dope," agents are less likely to interpret this as mere bragging or meaningless agreement, the agent said.[369] "[W]e are going to encourage the CI, keep talking to that guy and see if he's actually really doing those things," he stated, adding that the next step for agents regarding such people is to "[h]ave the CI make an arranged transaction, order up an ounce of meth, order up a firearm."[370]

In other words, an individual whom databases showed as having a criminal record would be further targeted to see if they would be willing to engage in a new crime that could lead to an arrest – while those not linked to criminal histories were left alone.

"[O]nce the [informants] meet people, they provide the information to us, and we try to weed out who is the worst of the worst walking the streets, and those are the ones we push the [informants] to try to arrange the transaction," the agent testified.[371] It was a criminal record that could lead

365 *United States v. Coleman and Jackson*, Memorandum Opinion and Order (doc. 73), February 7, 2018, at *7.

366 Ibid. at *7-8.

367 *United States v. Coleman and Jackson*, Transcript of Proceedings (doc. 62), November 18, 2017, pp. 17-18.

368 *United States v. Casanova*, Transcript of Motion Hearing (doc. 51), April 5, 2017, pp. 64-65.

369 Ibid. at p. 65.

370 Ibid, at p. 66.

371 Ibid. at p. 77.

a person to be designated as "the worst of the worst," he said, meaning that even a person who attempted to arrange a sale of a significant amount of methamphetamine would not be further investigated if they "had no real criminal history."[372]

When asked by the presiding judge, "Were there any written guidelines that defined who were the worst of the worst?", the agent replied, "No, sir."[373] No records were kept of decisions not to pursue an individual for further investigation.[374] The agent also testified that he had not received any training regarding implicit bias and that the confidential informants used during the "Surge" also had not received any such training.[375]

In the United States in 2010 (the most recent year for which we could find information at the time of writing), of the eight percent of the total US population with felony convictions, 33 percent were Black males.[376] As a range of US civil rights organizations have documented, Black adults in the US are disproportionately likely to be arrested for drug possession and are more likely to be incarcerated generally.[377] Statistics such as these suggest that Black adults are more likely than white adults to have a criminal record.

These higher arrest and conviction rates for Black Americans are not a result of any greater inclination among this group to commit crimes. A 2018 report by the Vera Institute of Justice concluded that "[b]ias by decision makers at all stages of the justice process disadvantages black people," whom evidence suggests are "more likely to be stopped by the police, detained pretrial, charged with more serious crimes, and sentenced more harshly than white people."[378] While the Sentencing Project suggests that "concentrated urban poverty" can be a risk factor for participation in some types of crime among Black Americans who live in such environments, the organization also points out that US police have "disproportionate levels of … contact with African Americans," which can result in members of this group being arrested more frequently for offenses that Americans of all races commit at similar rates, such as drug crimes.[379]

In turn, these patterns of policing and prosecution could lead Black and other minority Americans to have more significant criminal records in databases such as NCIC.

---

372 Ibid. at p. 80.

373 Ibid. at p. 82.

374 Ibid. at p. 85.

375 *United States v. Coleman and Jackson*, Transcript of Proceedings (doc. 72), January 8, 2018, pp. 252-253.

376 Alan Flurry, "Study estimates U.S. population with felony convictions," *UGA Today*, October 1, 2017, https://news.uga.edu/total-us-population-with-felony-convictions/ (accessed October 24, 2024); The Sentencing Sproject, "U.S. Criminal Justice Data", no date, https://www.sentencingproject.org/research/us-criminal-justice-data/ (accessed October 24, 2024).

377 E.g. Human Rights Watch, *Every 25 Seconds* (2016), pp. 4-5, https://www.hrw.org/report/2016/10/12/every-25-seconds/human-toll-criminalizing-drug-use-united-states (accessed October 24, 2024).

378 Elizabeth Hinton, LeShae Henderson and Cindy Reed, "An Unjust Burden: The Disparate Treatment of Black Americans in the Criminal Justice System", *Vera Institute of Justice*, May 2018, https://www.vera.org/downloads/publications/for-the-record-unjust-burden-racial-disparities.pdf (accessed October 24, 2024).

379 The Sentencing Project, "Report to the United Nations on Racial Disparities in the U.S. Criminal Justice System", April 19, 2018, https://www.sentencingproject.org/publications/un-report-on-racial-disparities/ (accessed October 24, 2024); The Sentencing Project, "Shadow Report to the United Nations on Racial Disparities in Sentencing in the United States", July 14, 2022, https://www.sentencingproject.org/policy-brief/shadow-report-to-the-united-nations-on-racial-disparities-in-sentencing-in-the-united-states/

Research has also repeatedly shown that US criminal history records may be inaccurate.[380] Yet, the ATF in Albuquerque relied heavily on these records as indicators of the likelihood that a person might currently be engaged in criminal activity.

The results of the ATF's investigative approach, which depended extensively on searches of databases that did not require any fact-based suspicion of wrongdoing, were stark. For example, a court opinion noted that at the time of the Albuquerque ATF "Surge," 3.4 percent of the city's population was Black – but during the Surge, the ATF arrested Black suspects at nearly eight times that rate.[381]

After hearing testimony, the judge presiding over defendant Yusef Casanova's trial found that "the methods used by the ATF in conducting this operation were likely to lead to a higher percentage of minority defendants" and that the ATF had "declined to make use of any policies or training designed to counteract that effect."[382]

However, Casanova's efforts to obtain the dismissal of the charges against him due to selective (i.e., biased) law enforcement were rejected in 2019, and Casanova was convicted of distributing methamphetamine and being a felon in possession of a firearm.[383]

Despite these outcomes in court, the ATF's use of NCIC, and potentially private-sector databases, to search for personal information and thereby select "the worst of the worst" among individuals the informants encountered in Albuquerque raises serious questions about the potential for databases to facilitate policing that disproportionately impacts people of color. There was no legal requirement for agents to show any fact-based reason for suspecting someone of being involved in a crime before searching the database to see if the person had a past criminal record and selecting targets for further investigation accordingly.

---

380 See Wayne A. Logan & Andrew Guthrie Ferguson, "Policing Criminal Justice Data," *Minnesota Law Review*, vol. 101 (2016), pp. 560-561.

381 *United States v. Casanova*, Order Granting Discovery (doc. 57), June 12, 2017, p. 2. The defense provided these statistics, which the government did not contest (at pp. 2-3).

382 *United States v. Casanova*, Order Granting Discovery (doc. 57), June 12, 2017, p. 4.

383 *United States v. Casanova*, Memorandum Opinion and Order (doc. 146), February 11, 2019, pp. 1-2; Jury Verdict (doc. 218), April 25, 2019.

Even when confidential informants reported that a person had made statements about being involved in crime, ATF testimony indicates that agents treated these statements, by default, as not amounting to credible evidence of actual involvement – unless NCIC then displayed a criminal record associated with the person's name.

Agents were thus able to access database information about people instantly, without meeting any legal criteria, and make decisions based on what they found. If there had been greater rights-protecting restrictions on their database access, such as a legal requirement for fact-based reasonable suspicion that someone was committing a crime, the agents may have investigated informants' contacts more thoroughly before deciding whom to prioritize. Their decision-making may then have carried less risk of arbitrariness and racially disproportionate impact.

Instead, the databases put information at officers' fingertips that could – and, defense attorneys argued, did – skew the pool of investigative subjects based on race.

Throughout the proceedings, ATF personnel rejected the possibility that their decisions had been influenced by race.

D. “Electronic peeping Toms”: Searches for women’s data

One of the most common allegations in the lawsuits and criminal cases we examined regarding police misuse of databases was improper searches for – or misuse of – data about women on the basis of sexual interest. Women’s partners have also allegedly been the targets of inappropriate database searches by officers.

Some of these searches have been linked to officers’ targeting, or alleged targeting, of women for other forms of mistreatment.

Police forces, legislatures, and companies have long had reason to be aware of these problems – not least because police have repeatedly been criminally prosecuted for misusing their database access to look up women’s information.

In Illinois, a police sergeant was convicted in 2008 of crimes including aggravated sexual assaults; he had previously looked up three of the victims — and in two cases, their family members — in LEADS, NCIC, or other law enforcement databases.[384] In Ohio, an officer was criminally convicted in 2017 of using that state’s LEADS database to carry out unlawful searches regarding a woman he was simultaneously convicted of stalking.[385] More controversially, a New York officer was convicted in 2013 of exceeding his authorization to access a federal database after searching NCIC for personal information about a female acquaintance in the context of elaborate sexual fantasies, although a federal appeals court reversed the conviction in 2015 after concluding that the lower court had construed the Computer Fraud and Abuse Act too broadly.[386]

384 *People v. Pelo*, 404 Ill. App. 3d 839 (2010).

385 *State v. Garn*, 91 N.E.3d 109 (2017).

386 *United States v. Valle*, 807 F.3d 508, 512-513, 525-528 (2nd Cir. 2015); *United States v. Valle*, 301 F.R.D. 53, 109-110 (S.D.N.Y. 2014).

In Alabama, one police chief testified in 2013 that he had encountered wrongful access to data in NCIC – including women’s data – frequently, stating that “[t]here’s a number of police officers, NCIC operators, 911 operators over the years that either got fired or prosecuted” for looking up license plate numbers (“tags”) for personal reasons, including “officers running tags to find out what cute girl is driving this car.”[387]

In addition to prosecutions, numerous civil lawsuits alleging police database searches for information about women or their partners, without a law enforcement purpose or otherwise improperly, have been filed for years throughout the United States. The rates at which officers carry out improper sexual- or gender-based searches are unknown, but the cases described below suggest to us that the problem occurs and that existing restrictions have not been sufficient to prevent it.

387 Documentation on file with the authors; the case is discussed in anonymised form as “C.S.” below. 911 is the telephone number used in the United States to call for emergency law enforcement, medical, or fire department assistance. The police chief was indicating that such database misuse is taken seriously.

Jane Doe, a sexual abuse survivor

According to allegations explained in a judicial opinion, a local officer made contact with a woman suffering from heroin addiction in South Carolina in 2014, telling her he had looked her up in a police database and “knew of her arrest history as well as her sexual abuse as a child.” The court described claims that during the subsequent months, the officer sexually assaulted the woman, “asked [her] to participate in fights with other women, touched her inappropriately many times, and drove her to buy heroin in his police vehicle.”[388]

The officer was later prosecuted, although he died during proceedings.[389] The woman’s lawsuit – which concerned the actions of his superiors and the municipality, all of which denied wrongdoing – appears to have resulted in a settlement regarding some defendants, and resulted in a jury award of $500,000 to the plaintiff in her case against the defendant police department in 2022.[390]

388 *Jane Doe-4 v. Horry County, South Carolina et al.*, case no. 4:16-cv-03136 (D.S.C.), Memorandum Opinion and Order (doc. 69), February 28, 2019, pp. 2-3.

389 ABC4 News, “Coroner: Former SC detective charged with misconduct, found dead of natural causes,” updated version of November 14, 2018, https://abcnews4.com/news/local/former-hcpd-detective-charged-with-misconduct-found-dead.

390 *Jane Doe-4 v. Horry County, South Carolina et al.*, Stipulation of Dismissal (doc. 108), July 9, 2019; Jury Verdict (doc. 193), May 9, 2022.

N.B.

"This is an absolute example of why this kind of information should not be accessible and how it could be abused and misused."

N.B., a woman living in a western US state, has argued in court that she became involved in a romantic relationship with a man who claimed to be a member of the Central Intelligence Agency and the Army Special Forces — but was actually a local police officer. As part of his deceptive story, in late 2014 the officer allegedly showed N.B. a "book report" he had compiled about her that included "several pages of personal information … including her driver's license and Social Security card," a federal court later wrote.[391] (The court described the officer's "conduct" as "deeply troubling"; however, the extent to which the court accepted N.B.'s specific claims about the officer's behaviors is unclear, and the reader should be aware that those claims remain allegations rather than established facts.)

When N.B. discovered the officer's true identity, she filed complaints with his department, and he resigned while under investigation for accessing N.B.'s information. However, the federal court ultimately dismissed N.B.'s claims, finding that since the officer's alleged behaviors were part of a personal relationship with N.B. rather than his official duties, constitutional protections did not apply.[392]

"We couldn't get the judge past seeing this as a personal issue, which is not unusual when it's issues involving the invasion of privacy of a woman, frankly," N.B.'s attorney, now deceased, told us in a 2018 interview. "The relationship element of this [meant] it was seen as a personal conflict, not a constitutional issue."

"This is an absolute example of why this kind of information should not be accessible and how it could be abused and misused," the attorney added. When asked whether requiring a warrant for police searches of databases of personal information would address the risk of abuse, the attorney replied, "It's not enough. I think it's a start, but I think there needs to be a serious look at what databases are out there, whether they should be out there in the first place, and how they're being used."[393]

391 Documentation on file with the authors. The information in this case is a matter of public record, but the authors are withholding N.B.'s full name in this report to avoid compounding the privacy intrusions N.B. experienced.

392 Ibid.

393 Interview with attorney for N.B., by telephone, July 3, 2018.

Anne Rasmusson, Alix Kendall, and other Minnesota plaintiffs

"The window-peepers of the electronic data age"

A string of federal lawsuits brought in Minnesota since 2012 also illustrate the possibility that officers will misuse their database access to violate women's privacy rights extensively, as allegedly occurred in those cases.

In 2007, former Saint Paul police officer Anne Rasmusson grew suspicious of officers who, she later claimed, expressed romantic interest in her and had already learned where she lived.[394] When Rasmusson requested an audit of searches for her driver's license data, as Minnesota law enabled her to do, the results led to a claim that police in more than a dozen departments had looked up her photograph and other data over 500 times.[395] As noted in section III(A)(ii) above, police searches of driver's license data without a legitimate government purpose are unlawful under the federal DPPA.

Rasmusson's 2012 lawsuit led to settlements totaling more than $1 million, with media reporting that officers' interest in her had stemmed from changes in her appearance.[396]

In the wake of Rasmusson's case, a range of Minnesotans, from other police officers to local members of the media and politicians, requested audits of searches for their driver's license data and allegedly discovered that police had accessed their information numerous times.[397] Several of these individuals were women who ultimately brought suits claiming that police had looked up their data due to romantic interest or for other inappropriate gender-based reasons.[398]

---

394 *Rasmusson v. Chisago County et al.*, case no. 0:12-cv-00632 (D. Minn.), First Amended Complaint (Third Revision) (doc. 90), March 15, 2013, p. 7.

395 Ibid. at pp. 8-9; Minnesota Statute 13.03(3).

396 Kim Zetter, "Female Cop Gets $1 Million After Colleagues Trolled Database to Peek at Her Pic," *Wired*, November 5, 2012, https://www.wired.com/2012/11/payout-for-cop-database-abuse/ (accessed October 24, 2024).

397 See, e.g., *Engebretson v. Aitkin County et al.*, case no. 0:14-cv-01435 (D. Minn.), Memorandum Opinion and Order (doc. 170), September 26, 2016, pp. 1-2; *Heglund et al.* v. City of Grand Rapids et al., 871 F.3d 572, 575-576 (8th Cir. 2017); *Porter v. City of Brooklyn Park et al.*, case no. 0:14-cv-00253 (D. Minn.), Complaint (doc. 1),

398 See, e.g., *Engebretson v. Aitkin County et al.*, Memorandum Opinion and Order, September 26, 2016, pp. 2-3; *Heglund et al. v. City of Grand Rapids et al.*, 871 F.3d 572, 575-576 (8th Cir. 2017).

At the upper end of the spectrum, Minneapolis-Saint Paul morning news host Alix Kendall discovered that her driver's license data had been searched nearly 4,000 times; another female news anchor alleged that her records had been searched 1,380 times.[399]

Kendall's complaint in her civil suit used the language not only of abuse of power, but also consent: an effort by police and other local authorities to "unlawfully peak behind the curtain of [her] private life ... without her knowledge or consent." The defendants, the complaint alleged, were "the window-peepers of the electronic data age"—implicitly drawing an analogy between these alleged privacy violations and sexual ones.[400]

Kendall's case, and others brought by both women and men against a range of Minnesota police and public authorities, resulted in opinions by the Eighth Circuit Court of Appeal that dismissed the allegations against some defendants while allowing others to proceed. Part of the difficulty for plaintiffs such as Kendall was that the appellate court examined each instance of access (or accesses occurring during narrow time frames) and, in most cases, decided that it was not suspicious or did not reflect a potential conspiracy.[401] For the court, the question was not the larger picture of police forces across the state looking up the private data of individuals without any established reason; it was the smaller picture of whether the plaintiff could show that any particular access or closely related set of accesses had violated constitutional rights. Unlike, for example, the judge in Jamison (see above), the Eighth Circuit focused on specific police rather than "the police"—or, to put it differently, the trees and not the forest. Time will tell whether other federal appellate courts decide to take the same view, but the specter of hundreds or thousands of police and other public authorities—in hundreds or thousands of rooms or squad cars across the state—deciding to look up the ID photos and other private data of news anchors, radio broadcasters, journalists, former beauty pageant winners, fellow officers, or wives of fellow officers (all of which describe plaintiffs in the Eighth Circuit case), for no clear reason, points to disturbing cultural norms that are not consistent with equality or human dignity.

399 Adam Belz, "Minneapolis to pay $193K to settle TV anchor's snooping case," *Star Tribune*, May 11, 2018, http://www.startribune.com/minneapolis-to-pay-193k-to-settle-tv-anchor-s-snooping-case/482319431/ (accessed February 5, 2026); Randy Furst, "KSTP-TV anchor has her driver's license data searched 1,380 times, lawsuit alleges," *Star Tribune*, September 17, 2013, http://www.startribune.com/kstp-anchor-s-license-data-was-snooped-1-380-times-suit-says/224004771/ (accessed February 5, 2026).

400 *Kendall v. City of Albert Lea et al.*, case no. 0:14-cv-00247 (D. Minn.), Complaint (doc. 1), January 26, 2014, pp. 4-5.

401 E.g., Tichich et al. v. City of Bloomington et al., 835 F.3d 856 (8th Cir.), September 1, 2016.

Cyndi Thibault and Claude Letourneau

Suits alleging improper lookups of driver’s license data belonging to women or their partners extend beyond Minnesota. In Florida in 2016, a random audit of police use of the state’s Driver and Vehicle Information Database (“DAVID”) showed that a female officer had looked up the driver’s license information of her fiancé’s ex-wife, Cyndi Thibault, as well as Thibault’s husband Claude Letourneau, scores of times. The officer later admitted to looking up the data without a law enforcement purpose, and the court rendered judgment in favor of the couple.[402]

The case concerned one of many reported episodes in Florida of alleged improper searches by police and other officials for individuals’ information in DAVID, although authorities have sometimes claimed that the searches were conducted for legitimate purposes and the state’s Department of Highway Safety and Motor Vehicles has described adding a warning against misuse to the database interface.[403]

402 *Letourneau et al. v. Carpio*, case no. 0:17-cv-60082 (S.D. Fla.), Order on Summary Judgment (doc. 57), December 5, 2017, pp. 2-3; Final Judgment (doc. 115), July 18, 2018.

403 See, e.g., Lynnsey Gardner et al., “I-TEAM: Unauthorized searches made on law enforcement databases,” *News4Jax*, July 3, 2017, https://www.news4jax.com/news/investigations/i-team-unauthorized-searches-made-on-law-enforcement-database (accessed October 24, 2024); Howard Altman, “Misuse of state’s driver database often for personal reasons,” Tampa Bay Times, August 27, 2016, https://www.tampabay.com/news/publicsafety/states-driver-database-ripe-for-misuse/2291246 (accessed October 24, 2024); Dave Elias, “Deputy fired for misusing driver’s license database,” NBC2, April 24, 2014, https://www.nbc-2.com/story/25334275/deputy-fired-for-improperly-accessing-info-about-governor-nbc2-anchors-others (accessed August 12, 2019); Amy Pavuk, “Law-enforcer misuse of driver database soars,” Orlando Sentinel, January 22, 2013, https://www.orlandosentinel.com/news/os-xpm-2013-01-22-os-law-enforcement-access-databases-20130119-story.html (accessed August 12, 2019).

What went wrong

These established and alleged improper police searches for data about women, including female fellow officers and current and former romantic partners, are foreseeable consequences of making large collections of personal information easily available to officers. The cases described above establish that law enforcement databases provide a tempting pool of information, particularly for those officers who are or may become perpetrators of stalking or other gender-based abuse.

We therefore agree with N.B.’s attorney that this documented and alleged database misuse fundamentally stems from the availability of the data to police, as well as a seeming failure on the part of government agencies and companies to make the possibility of gender-based abuse and the possibility of misogyny among officers a central consideration when deciding whether to offer or purchase access to large collections of personal data.

E. Queries concerning fellow officers

i. Amy Krekelberg: A showdown in Saint Paul

"Officers frankly goofed off with the database system."

In a striking scene, the jury in a civil trial that one of the authors of this report observed in June 2019 watched police officers enter the court and take seats at both the plaintiff's and defendants' tables. More than five years earlier, officer Amy Krekelberg of the Minneapolis Police Department had filed a lawsuit against a range of municipalities after obtaining records allegedly showing that her fellow officers had looked up her data in the state's driver's license database nearly 1,000 times.[404] The information included her photograph, height, weight, birthdate, and home address.[405]

Krekelberg argued that her Minneapolis colleagues had searched for her driver's license data 87 times between 2009 and 2012 without any policing purpose, violating the DPPA.[406]

In court, Krekelberg described her suit as an effort to defend women's rights. "As a female, I think it's important … I hope this changes the way the Minneapolis Police Department does business with its female officers," she testified, adding, "I think we need to be taken seriously, and I want to be taken seriously as a police officer."[407]

---

404 *Krekelberg v. Anoka County et al.*, case no. 0:13-cv-03562 (D. Minn.), Complaint (doc. 1), December 17, 2013, para. 274.

405 Direct examination of Kim Jacobson, Minnesota Department of Public Safety, United States District Court for the District of Minnesota (Saint Paul), observed in person, June 11, 2019; see also *Krekelberg v. Anoka County et al.*, Plaintiff's Statement of the Case (doc. 630), May 2, 2019, pp. 1-2, although Jacobson testified during cross-examination that officers could not view Social Security numbers by looking up driver's license information in the database.

406 *Krekelberg v. Anoka County et al.*, Plaintiff's Statement of the Case (doc. 630), p. 3.

407 Direct examination of Amy Krekelberg, officer, Minneapolis Police Department, United States District Court for the District of Minnesota (Saint Paul), observed in person, June 12, 2019.

Krekelberg also testified that learning of the numerous searches resulted in several psychological harms and physical symptoms.[408] She further alleged that after filing her lawsuit, she was socially ostracized at work and feared fellow officers would no longer respond to any calls she might make for emergency backup (a concern the city of Minneapolis, which represented the police department in the lawsuit, vigorously disputed).[409]

Attorneys for the city responded in part by noting that Krekelberg herself had carried out unauthorized searches of driver's license data earlier in her career.[410] The city's attorneys also rejected the idea that someone could suffer emotional harm from the needless viewing of her driver's license data. One attorney for the city pulled his own driver's license from his wallet and displayed it to the jury on a large screen to suggest that license information is not sensitive.[411]

The city also argued at the beginning of the trial that Krekelberg had not experienced any actual harm. "None of these officers stalked her … nobody drove past her house, nobody stole her identity," an attorney said. "Some Minneapolis police officers looked at her driver's license info. That's it."[412]

"Officers frankly goofed off with the database system" across the state at the time, he added, citing a lack of training that he said has since been remedied.[413]

At the trial's conclusion, the jury found that the searches of Krekelberg's data by Minneapolis police had been illegal and awarded Krekelberg $585,000 in actual and punitive damages.[414] However, in 2021, the Eighth Circuit Court of Appeal found that the trial court had abused its discretion by allowing the plaintiffs to introduce certain evidence at trial and that the jury instructions had been flawed; it vacated the previous judgment, remanding the case for a new trial.[415] The case ended in a settlement before the new trial could occur.[416]

---

408 Ibid.

409 Ibid.; cross-examination of Amy Krekelberg, United States District Court for the District of Minnesota (Saint Paul), observed in person, June 12, 2019. The city of Minneapolis also elicited testimony from other witnesses disputing the claim that officers would have been reluctant to provide Krekelberg with backup, e.g., direct examination of Jennifer Lazarchic, officer, Minneapolis Police Department, United States District Court for the District of Minnesota (Saint Paul), observed in person, June 12, 2019.

410 Cross-examination of Amy Krekelberg by city of Minneapolis, United States District Court for the District of Minnesota (Saint Paul), observed in person, June 12, 2019.

411 Cross-examination of Kim Jacobson, Minnesota Department of Public Safety, by city of Minneapolis, United States District Court for the District of Minnesota (Saint Paul), observed in person, June 11, 2019.

412 Opening argument, city of Minneapolis, United States District Court for the District of Minnesota (Saint Paul), observed in person, June 10, 2019.

413 Ibid.

414 Human Rights Watch, "US: Police Found to Violate Fellow Officer's Privacy," June 20, 2019, https://www.hrw.org/news/2019/06/20/us-police-found-violate-fellow-officers-privacy (accessed October 24, 2024).

415 *Krekelberg v. City of Minneapolis et al.*, 991 F.3d 949 (8th Cir.), March 19, 2021.

416 *Krekelberg v. City of Minneapolis et al.*, Order on Motion for Attorney Fees (doc. 926), July 27, 2023, p. 4.

ii. Other alleged searches for data belonging to fellow officers, justice professionals, and public safety personnel

Krekelberg's case, and Rasmusson's from the preceding section, are not the only ones in which US police officers allegedly misused their access to large collections of personal data to peer into the lives of fellow police, public safety personnel, and criminal justice professionals. We have located more than a dozen federal lawsuits by such individuals since 2009.

A large proportion of these suits concerning fellow officers and people in closely connected professions were brought in Minnesota and concerned searches for driver's license data. As noted above, Minnesota state law empowers individuals to request audits of the number of times authorities have looked up their information in the database, and the well-publicized 2012 suit by former officer Anne Rasmusson (see section IV(D)) may have helped inspire the other claims. Greater rights of access to information about officers' searches for data, if established in other states, might lead to revelations of similar problems.

D.W.

Female highway patrol officer D.W. has said she pulled over an off-duty police officer for speeding and ticketed him during a tense encounter in a state in the US south in late 2011.[417] She later alleged in a lawsuit that following this traffic stop, she was subjected to hang-up calls and other harassment.[418]

Eventually, D.W. discovered that more than 80 individual officers had looked up her personal information in the state's DAVID database.[419] Although some of D.W.'s claims were resolved through settlements and several of the officers who had searched for her data received official reprimands, a federal appeals court rejected her claims against these officers in 2017, finding she had not shown that they had clearly violated the DPPA when they looked her up.[420]

As a result of these events, D.W. has suffered online abuse. In late 2015, one commenter on an unofficial forum intended for law enforcement – whose comment continued to feature prominently in Google search results for information about and commentary about the lawsuit several years later – criticized D.W.'s weight and age, asked if she'd received a settlement, and expressed violent sentiments.[421]

Regardless of whether any of these commenters were in fact police officers, their comments continue to form part of D.W.'s online reputation.

417 Documentation on file with the authors. Although the records from this lawsuit were publicly filed, we are using initials for D.W. to avoid reigniting the online abuse they have suffered surrounding their case.

418 Documentation on file with the authors.

419 Documentation on file with the authors.

420 Documentation on file with the authors.

421 Documentation on file with the authors.

An Alabama officer and his romantic partner

At a police department in Alabama, a slip of paper appeared on a cabinet one day in 2012 bearing a Social Security number and a brief note suggesting the number was associated with a felony. When a curious officer searched for the number in law enforcement databases containing personal information, he discovered that it belonged to a fellow officer's romantic partner – C.S., a woman – and that C.S. had a criminal record.[422]

Other officers then accessed or viewed C.S.'s data, and the police chief pressured her partner to end the relationship due to C.S.'s past convictions.[423] When the officer refused to break up with C.S., he was fired.[424]

C.S. sued, alleging that the database searches and sharing of her information had violated her constitutional and other privacy rights. The court found that the searches for her data had not been lawful, but that she had not had a protected privacy interest in the data under the Constitution. On these and other grounds, her lawsuit was dismissed.[425]

422 Documentation on file. Although the records from this lawsuit were publicly filed, we are using initials for C.S. because the allegations were related to an intimate relationship and because we wish to avoid perpetuating the harm that occurred.

423 Ibid.

424 Ibid.

425 Ibid.

What went wrong

Several of the cases we examined indicate that even when federal law prohibits officers from looking up certain personal data without a legitimate purpose, these prohibitions may not be effective if a police department's culture or practices do not effectively discourage and punish such behavior. Krekelberg's case also prompts specific concerns about gender-based lookups of female fellow officers and criminal justice professionals – actions that do not treat female colleagues as respected equals.

F. Searches due to political activities or for retaliation

Several plaintiffs have alleged in federal court that officers unlawfully looked up their data due to their political activities or a desire to retaliate against them.

Most significantly, in a 2013 Wyoming incident that a federal appeals court has described as stemming from "a feud between city leaders," it was claimed that a police chief instructed his subordinate to search TLOxp for information about a city council member in an effort to establish whether the man truly lived in the district he represented – as he had asserted in a sworn statement and as was required.[426] The council member in question sued, claiming that some of the data the officer had retrieved was protected under the DPPA but had been accessed without a legitimate purpose, violating his rights. The appeals court found in 2019 that the evidence – viewed in the light most favorable to the city council member who had brought the suit – suggested the police chief had simultaneously had the "permissible" goal of investigating the possible crime of making a false sworn statement, and "an impermissible purpose of unseating a political rival for reasons unrelated to a legitimate investigation." (In other words, as the court put it, a "political vendetta.") Over a dissent, the court went on to find that since at least one of the police chief's purposes had been permissible, the chief had not clearly violated the law and was thus immune from suit.[427]

426 *Hedquist v. Walsh et al.*, 786 Fed. Appx. 130 (10th Cir.), August 23, 2019; *Hedquist v. Walsh et al.*, case no. 1:16-cv-00265 (D. Wyo.), Order (doc. 66), April 2, 2018, pp. 2-5.

427 *Hedquist v. Walsh et al.*, 786 Fed. Appx. 130.

A Florida police officer has similarly claimed that other officers looked up his driver's license information in the state's DAVID database from 2011 to 2012 without a law enforcement purpose while he was running for county sheriff.[428] The department denied these allegations, and the officer's lawsuit ended in a settlement in 2016.[429]

The factual records or motivations in these and a handful of other relevant cases are disputed or unclear. However, they point to the troubling possibility that – just as there is little to prevent officers from searching for data about women or minorities without a reasonable suspicion of wrongdoing – in practice, there may be equally little to prevent searches for damaging personal data in the context of political or personal disagreements. Such a practical ability would represent a large and dangerous power disparity between officers and individuals whom they may happen to dislike.

428 *Santarlas v. Minner et al.*, case no. 5:15-cv-00103 (M.D. Fla.), Second Amended Complaint (doc. 30), October 30, 2015, ¶¶ 32-34.

429 *Santarlas v. Minner et al.*, Defendants' Answer (doc. 42), March 10, 2016, ¶¶ 32-34; Order (doc. 48), July 26, 2016.

V.
Greater Data, Greater Risks: The Future

The cases described above illustrate human rights harms that stem from weak or nonexistent restrictions on the personal data that the government and private data brokers can gather and store about people in the US today – and on police access to that data.

Despite these concerns, digital collections of data about people grow ever more extensive, and systems for merging and mining that data to produce insights about our lives grow ever more powerful. It is therefore important for the US as well as other countries and international bodies (such as the EU) to consider not only the rights violations that are occurring now, but those that may worsen or emerge in the near future.

For example, the civil rights lawsuits – and, in some instances, related criminal prosecutions – described above often stemmed from access to data that many people in the United States and elsewhere might regard as relatively basic, such as address, license plate, phone number, photographs, and information about outstanding warrants. The easy availability of even this seemingly basic information has resulted in abuses.

At the same time, police have access to ever-more-sophisticated and sensitive data, such as facial recognition, other biometric data, and internet browsing information, including from both government and private-sector sources.

This phenomenon of lawmakers granting police ever-greater access to information about people is occurring even though the serious harms of warrantless police access to even relatively basic personal information have never been addressed. There appears to be a widespread assumption that greater police access to data is necessarily a benefit for public safety, even though this report suggests the opposite. Giving police increasingly comprehensive data about people, and increasingly sophisticated software to merge and mine that data, means handing a large amount of power to a group of people who often have little accountability in practice – and have a state-sanctioned ability to use force. The harmful consequences that have flowed from such decisions have been predictable. There is every reason to believe that those harms will increase as the access to data does.

Legislators in the US and elsewhere often have not passed laws quickly enough to keep up with new technologies, with the result that police access to personal data is often governed by laws or rules that are decades old. By looking to the foreseeable future now, lawmakers could break this pattern and impose more effective limits on what kinds of personal information police can view, when, and why.

A. Sensitivity, merging, and mining

As described in section III above, private data brokers based or active in the US already advertise that they can offer police access to data that goes far beyond the information that led to the abuses and alleged abuses described in this report.

Today, US police can purchase access to financial and social media information, map people's relationships and broader social networks, conduct facial recognition scans, and obtain location information using these private tools – and the depth and sensitivity of the personal data available from these sources are likely to increase as data brokers compete with one another for the law enforcement market. Combined with social media intelligence ("SOCMINT") software[430] and facial recognition/online surveillance software such as Clearview AI's,[431] the level of privacy intrusion that this data enables will continue to grow exponentially.

Meanwhile, US federal and state databases also include an ever-increasing and potentially consequential range of personal information, such as biometric data, purported gang affiliation, and "propensity to be violent toward law enforcement."

Just as the range and depth of personal data available to police continue to grow, so, too, does the technical ability to merge and mine this information for far-reaching insights into people's relationships and private lives. The continuing development of such analytic tools means that police will have ever-growing abilities to fuse and analyze seemingly non-revealing information to create sophisticated pictures of personal life.

430 See Privacy International, "The use of social media monitoring by local authorities – who is a target?," May 24, 2020, https://privacyinternational.org/explainer/3587/use-social-media-monitoring-local-authorities-who-target.

431 Privacy International, "Challenge against Clearview AI in Europe," https://privacyinternational.org/legal-action/challenge-against-clearview-ai-europe.

In the future, an increasing number of police departments around the world are also likely to have access to software designed not just for the investigation of past alleged crimes, but the prediction of future ones. Several large departments in the US reportedly already use, or have experimented with, software tools for this type of "predictive policing."[432] The US federal government has also long expressed interest in algorithms to predict future behaviors or estimate dangerousness.[433]

Regardless of the specific types of personal data or predictive tools police and politicians embrace, the same risks and violations detailed in this report will continue unless governments adopt strong laws to prevent them.

---

432 See, e.g., Sidney Fussell, "The NYPD Had a Secret Fund for Surveillance Tools," *Wired*, August 10, 2021, https://www.wired.com/story/nypd-secret-fund-surveillance-tools/; Matt Stroud, "Heat Listed," *Verge*, May 24, 2021, https://www.theverge.com/c/22444020/chicago-pd-predictive-policing-heat-list; National Institute of Justice, *Program Profile: Predictive Policing Model in Los Angeles, Calif.*, November 28, 2022, https://crimesolutions.ojp.gov/ratedprograms/predictive-policing-model-los-angeles-calif#5-0.

433 See, e.g., Brennan Center for Justice, "ICE Extreme Vetting Initiative: A Resource Page," https://www.brennancenter.org/analysis/ice-extreme-vetting-initiative-resource-page (accessed August 31, 2019); but see Brian Root, "US Immigration Officials Pull Plug on High-Tech 'Extreme Vetting,'" Human Rights Watch, May 18, 2018, https://www.hrw.org/news/2018/05/18/us-immigration-officials-pull-plug-high-tech-extreme-vetting.

VI. Recommendations: Ending and Preventing Harms to Rights

We regard the confirmed and alleged rights harms detailed in the civil rights lawsuits described above, as well as the even more extensive harms that may occur in the future, as preventable. Legislatures, police forces, and courts should take steps now to curtail potentially abusive law enforcement access to personal data and ensure accountability for violations.

One reason legal change is important is that, as the outcomes of many cases described in this report show, the ability to sue law enforcement agencies and officers regarding alleged data abuses is not sufficient to ensure accountability. Even if the data access is not disputed, plaintiffs in the US are forced to contend with judicially established legal standards – such as those for overcoming officers' qualified immunity – that make it difficult to bring a successful civil rights claim against police.

For these and other reasons, lawmakers and courts should not expect that the ability to bring civil lawsuits against officers will be sufficient to prevent the misuse of personal information. Legal reforms are needed.

A. Collection and retention of the data

The protection of privacy and other rights in this area requires limits on what data is collected and retained.

We urge the adoption of comprehensive restrictions on the personal data that companies and government agencies can compile, store, buy, and (in the case of the private sector) sell.

We recommend the following:

1. Recognize that natural persons have a privacy interest in data that is, or can be, linked to them as identifiable individuals – regardless of whether they have previously shared the information with others, or whether it appears to be inherently sensitive.

2. Require a specific statutory authorization for all government compilation and storage of digitized personal data, and limit the government's storage of personal information in large, digitized collections to what is strictly necessary to achieve a legitimate aim.

3. Require government authorities to delete personal data that is outdated or no longer strictly necessary to achieving a legitimate aim, and require the correction of personal data that is incorrect (such as the wrongful linking of an individual with an outstanding warrant).

4. Prohibit the private sector from selling personal data, or access to such data, to police. Police should only be able to obtain such data from the private sector with a warrant or court order. There should be a firm limit on the private sector's collection and storage of personal data when the person has not specifically and knowingly consented to these activities.

B. Law enforcement access to the data

Many of the rights harms established or alleged in the cases described above resulted from insufficiently restricted police access to personal data that is stored in large systems, particularly the legal ability of police to look up personal information without any probable cause or even reasonable suspicion that someone had engaged in wrongdoing. Officers legitimately investigating offenses have also harmed rights after viewing personal information that was not directly or immediately relevant in the circumstances – sometimes because the data led them astray, and sometimes because they misused it.

To prevent crimes, police do not need the ability to look up the license plate of a driver who is simply parked near a shopping center, driving past an officer, or making a rapid turn, as allegedly occurred in cases described above.[434] To prevent serious crimes, they do not need an instant ability – everywhere and at all times – to see whether a bench warrant for an alleged theft has been issued, as was situation in the M.R. case above, or whether a warrant has purportedly been issued for someone merely suspected of jumping a subway turnstile, as allegedly occurred in another case we found during our research.[435] Nor do they need the practical ability to view women's – or men's – driver's license data without any suspicion of wrongdoing, as occurred in the Minnesota lawsuits described above. Most will not need automatic access to information about whether someone has been a victim of child sexual abuse – access that enabled a predatory officer to target the vulnerable Jane Doe in South Carolina.

434 *Tolan v. Cotton*, 572 U.S. 650, 651 (2014).

435 *Gaston v. Ruiz et al.*, case no. 1:17-cv-01252 (E.D.N.Y.), Complaint (doc. 1), March 6, 2017, pp. 6-7; Memorandum and Order (doc. 18), p. 3.

We recommend the following:

5. Require a warrant based on the Fourth Amendment standard of probable cause, a court order, or specific statutory authorization for police access to personal information in a government-run or private-sector database -- unless a recognized exception to the warrant requirement, such as the existence of a genuine emergency, applies.

6. Require police departments to refrain from granting officers the credentials or technical ability to gain access to personal data they do not require to perform their specific responsibilities, and ensure disciplinary action when such access occurs.

7. Establish that unauthorized police access to personal information necessarily causes harm to privacy rights, regardless of whether or how police later misuse that information.

8. Create a cause of action for civil lawsuits based on such unauthorized access.

9. Prohibit searches for personal information about individuals reporting crimes or seeking emergency help unless the situation provides probable cause to believe that the individual in question has committed or is committing a criminal offense.

10. Limit police access to records of an individual's prior encounters with law enforcement.

11. Require officers to provide a written justification in advance – except in a bona fide emergency – for every attempt to gain access to personal data from a digitized collection, and establish that the lack of a compelling written justification renders the search per se unreasonable.

12. Require police departments to log searches of personal data, whether conducted in government-run or private-sector databases, and carry out regular audits.

13. Clearly establish penalties for officers who violate rights or break the law when accessing, using, or handling personal data.

14. Require courts presiding over criminal trials to exclude database results, or evidence obtained thanks to such results, if officers' access to or treatment of the data violated rights or broke the law.

C. Presentation and correction of the data

The manner in which personal information is presented to officers in databases can cause rights harms. For example, the inclusion of names as potential "aliases," without an explanation of why an individual is linked to more than one name, can wrongly imply criminality and/or result in mistaken identity. The unnecessary presentation of photographs or other information indicating race can also invite implicit or explicit bias.

Evidence suggests that officers are aware that the data they obtain from databases may not be reliable. For example, as noted above, an ATF agent testified in a criminal case arising from the 2016 Albuquerque "Surge" operation freely stated that "NCIC is only as good as what people put into it" and that some of the information in the database is inaccurate.[436] Police departments should provide officers with regular and explicit training about the potential unreliability of database information – especially since it is easy to assume that technology is factual and objective, and therefore must be "right."

While police should receive greater training regarding the potential inaccuracy of database information and the risk of confirmation bias, courts should also recognize that it is not always reasonable for officers to rely on database information as if it were necessarily true, and that training alone will not necessarily solve the problem. The mistaken identity cases documented in this report, all of which were publicly filed and litigated, make it clear that officers know or should know that information found in databases may be inaccurate or misleading. In particular, officers are, or should be, aware of the risk that information concerning one individual may be wrongly linked to another. Database information alone, including information about the purported existence of a warrant, should not be regarded as sufficient evidence of probable cause for an

436 *United States v. Jackson,* case no. 1:16-cr-2362 (D. N.M.), Transcript of Proceedings, Vol. I (doc. 62), November 18, 2017, p. 109.

arrest, although it might provide "reasonable suspicion" in support of a brief detention (known in US legal parlance as a "Terry stop"[437]) while officers investigate whether the person in question is in fact the same as the person who is the subject of the warrant.

Regarding the potential inaccuracy of the data, we conclude that police departments and companies should be responsible for ensuring that the information in the systems is correct and up-to-date. In human rights terms, it is not acceptable to have a mess that no one is responsible for cleaning up.

We recommend the following:

15. Mandate that police may only gain access to personal information in databases if the databases provide clear information about the origin of the information and how recently it was updated.

16. Require regular audits to purge or correct information that is outdated or untrue.

17. Require other regular maintenance to ensure the accuracy of the information.

18. Create a cause of action against agencies and companies for failing to correct database information they have reason to know is inaccurate.

437 From *Terry v. Ohio*, 392 U.S. 1 (1968).

E. Transparency and accountability

The research presented in this report also reveals a need for far greater transparency about the personal data that is stored in government and private databases available to law enforcement – and how authorities can use that information.

Transparency alone will not be sufficient to prevent the rights harms that can stem from police access to personal information. Legislatures and courts should also consider whether a data collection's existence and purpose are justifiable in a rights-respecting society, whether there are documented or foreseeable risks of misuse, and whether existing safeguards are strong enough to prevent rights violations.

Greater transparency, while important for accountability and regulation, also should not serve as an excuse for shifting the burden of identifying and seeking the correction of inaccurate or outdated information onto the individual who is linked with the data. As people's information appears in an ever-increasing range of private-sector and policing databases, such a task becomes as impractical as it is distressing.

In addition to those detailed above, further measures are needed to create greater transparency regrading personal data availableto police.

We recommend the following:

19. Require government agencies and private companies to publish complete information about the types of personal data they hold, or to which they have access, and the provenance of that data. This information about the systems and their contents should be continually updated.

20. Empower individuals to view and obtain the correction and updating of personal data police hold in databases or to which they have access, with narrowly tailored exceptions where strictly necessary to achieving a legitimate government aim; and ensure that such exceptions are not applied in a way that prevents transparency or accountability in practice. Audits, corrections, updates, and other measures on the part of the data aggregator (whether government or private-sector) should still be required.

Conclusion

The lack of protections for data privacy in the United States is dangerous. It is dangerous for people of color. It is dangerous for women. It is dangerous for drivers, passengers, bystanders, and victims of crime. It is dangerous for both police and members of the public who find themselves in needless encounters with law enforcement. Ultimately, it is dangerous for everyone.

Until the United States adopts laws imposing far stronger safeguards for the personal data held in both government-run and private databases, the evidence strongly suggests that police access to this data will continue to result in or contribute to arrests and detentions based on mistaken identity; stalking and other gender-based harms to women; violations of the privacy of fellow officers; and suspicionless searches potentially based on racial bias or personal disputes. For people affected by these rights violations, the fallout can be devastating, including physical and psychological harms, damage to relationships, and an erosion of trust in public officials.

These harms are foreseeable, and as departments increasingly adopt other data-based policing methods, they could be magnified or appear in even more forms.

The recurrence or worsening of these rights violations must be prevented by limiting the types of personal data private companies and law enforcement can gather, store, share, and search; restricting access to the data; increasing oversight; remedying problems of inaccuracy and incompleteness; and mandating greater transparency.

It is not too late to address and prevent the harms of out-of-control personal data collection and access in the United States and around the world. The rights of people in the digital age demand such measures – and the years-long, nationwide history of abuse presented in this report makes it clear that there is no time to lose.

Back to Contents ↑