Policing Police Access to Criminal Justice Data

Wayne A. Logan[*]

ABSTRACT: Today, it is widely recognized that we live in an information-based society. This is certainly true of police on street patrol, who more than ever before rely on, and enjoy ready access to, information when doing their work. Information in aggregated form, for instance, is used to create algorithms for "hot spot" policing that targets specific areas. Information concerning individuals, however, must somehow be tied to them if it is to be useful. An arrest warrant in a database, for example, lies inert until an officer associates it with an individual; so too does information regarding suspected gang affiliation and the mass of other information contained in databases.

With databases expanding exponentially by the day, and police engaging in what has come to be known as database policing, in search of "hits," personal identity has assumed unprecedented importance. This Article addresses these developments. Unlike prior scholarship, which has focused mainly on the collection and use of information regarding individuals, the Article examines the intermediate step of database policing: the means by which police access database information. For police, the benefits of such access are as broad as the expanse of databases on which they have come to rely, which is very broad indeed.

Databases today include not only arrest warrants, most often for minor offenses, which police can use for evidentiary "fishing expeditions" when conducting searches incident to arrest. They also include records of prior stops, arrests, and convictions, which often reflect racially biased policing practices that are reified when relied upon by police. Databases even contain personally sensitive information that, while not incriminating, can be embarrassing for individuals who are detained. By conceiving of personal identity itself as evidentiary fruit worthy of constitutional regulation the Article fills a major gap in policing scholarship, addressing a matter that will only grow in importance as police rely on databases that are rapidly proliferating in number and kind.

---

[*] Gary & Sallyn Pajcic Professor of Law, Florida State University College of Law. Thanks to Jeff Bellin, Barry Friedman, Brandon Garrett, Rachel Harmon, Richard Re, Ric Simmons, Chirs Slobogin, Sam Wiseman, and Ron Wright for their very helpful suggestions.

I. INTRODUCTION 620

II. POLICE AUTHORITY TO ACCESS DATABASES 626
A. *ATTENUATION DOCTRINE* 628
B. *THE IDENTITY EXCEPTION* 635
C. *SUMMARY* 639

III. THE CONSEQUENCES OF POLICE ACCESS 640
A. *ARREST WARRANTS* 640
B. *OTHER DATABASES* 645
1. Stop, Arrest, and Conviction Records 645
2. Biometric Data 649
3. Unlawfully Secured Evidence 651
4. Sensitive Personal Information 653
C. *IMPLICATIONS* 655

IV. SKETCHING THE PATH AHEAD 661
A. *CLEARING AWAY THE DOCTRINAL UNDERBRUSH* 661
B. *DOCTRINAL PATHS* 664
1. Fourth Amendment 664
2. Fifth Amendment 669
3. Remedy 671
C. *STATUTORY FIX* 673

V. CONCLUSION 676

I. INTRODUCTION

"What's in a name? That which we call a rose

By any other name would smell as sweet . . . ."[1]

While the Immortal Bard today justly remains one of history's most astute observers of human society, it turns out that he was wrong in his assessment of the importance of personal identity. As society has become increasingly information-based, identity has come to play an ever more critically important role. This is especially so with policing, where knowing who a person is affords access to a vast network of databases permitting officers to search, seize, surveil, and question individuals.

1. WILLIAM SHAKESPEARE, THE TRAGEDY OF ROMEO AND JULIET, act 2, sc. 2, ll. 43–44 (Daniel Fischlin ed., 2013).

In Chicago, for instance, knowledge of personal identity affords police access to a "Strategic Subject List"[2] and a "[H]eat [L]ist" containing risk analyses of individuals believed likely to be involved in future violence.[3] In New York City, police, as in many other locations, maintain a list of suspected gang members,[4] and also utilize a "Domain Awareness System" that assembles and links information from multiple sources, such as video surveillance, license plate readers, and arrest records.[5] Boston police collect and store observational "data on the activities and whereabouts of known and suspected criminals and their associates."[6] Meanwhile, data "fusion centers" nationwide combine and analyze data from multiple sources,[7] including private businesses[8] and household devices comprising the "Internet of Things."[9]

Police also rely upon more traditional databases containing arrest warrants and information regarding prior stops, arrests, and convictions,[10] and biometric information such as fingerprints and DNA, resulting in what Justice Scalia has called a "genetic panopticon."[11] No less significant, databases often contain information of a highly sensitive nature, which while

2. Mick Dumke & Frank Main, *A Look Inside the Watch List Chicago Police Fought to Keep Secret*, CHI. SUN-TIMES (May 18, 2017, 9:26 AM), https://chicago.suntimes.com/news/what-gets-people-on-watch-list-chicago-police-fought-to-keep-secret-watchdogs.

3. Monica Davey, *Chicago Police Try to Predict Who May Shoot or Be Shot*, N.Y. TIMES (May 23, 2016), https://www.nytimes.com/2016/05/24/us/armed-with-data-chicago-police-try-to-predict-who-may-shoot-or-be-shot.html; Jeremy Gorner, *Chicago Police Use 'Heat List' as Strategy to Prevent Violence*, CHI. TRIB. (Aug. 21, 2013), http://articles.chicagotribune.com/2013-08-21/news/ct-met-heat-list-20130821_1_chicago-police-commander-andrew-papachristos-heat-list.

4. *See* K. Babe Howell, *Gang Policing: The Post Stop-and-Frisk Justification for Profile-Based Policing*, 5 U. DENV. CRIM. L. REV. 1, 15–16 (2015).

5. Rocco Parascandola & Tina Moore, *NYPD Unveils New $40 Million Super Computer System that Uses Data from Network of Cameras, License Plate Readers and Crime Reports*, N.Y. DAILY NEWS (Aug. 8, 2012, 8:50 PM), http://www.nydailynews.com/new-york/nypd-unveils-new-40-million-super-computer-system-data-network-cameras-license-plate-readers-crime-reports-article-1.1132135. *See generally* Christopher Slobogin, *Panvasive Surveillance, Political Process Theory, and the Nondelegation Doctrine*, 102 GEO. L.J. 1721 (2014) (surveying wide variety of "panvasive surveillance" techniques employed by police).

6. Jeffrey Fagan et al., *Stops and Stares: Street Stops, Surveillance, and Race in the New Policing*, 43 FORDHAM URB. L.J. 539, 547 (2016) (quoting Bos. Police Dep't, Special Order SO 05-023, June 3, 2005, § 1).

7. *See, e.g.*, *National Network of Fusion Centers Fact Sheet*, U.S. DEP'T HOMELAND SECURITY, https://www.dhs.gov/national-network-fusion-centers-fact-sheet (last updated Aug. 14, 2018) (describing centers as "focal points . . . for the receipt, analysis, gathering, and sharing of threat-related information [between the] federal [government and] state, local, tribal, and territorial [and private sector] partners").

8. Chris Jay Hoofnagle, *Big Brother's Little Helpers: How ChoicePoint and Other Commercial Brokers Collect and Package Your Data for Law Enforcement*, 29 N.C. J. INT'L L. & COM. REG. 595, 621–22 (2004).

9. *See generally* Andrew Guthrie Ferguson, *The "Smart" Fourth Amendment*, 102 CORNELL L. REV. 547, 554–60 (2017) (discussing how smart devices record data on human behavior and intentions that can be used by law enforcement).

10. For a comprehensive treatment of the role played by criminal records more generally, see JAMES B. JACOBS, THE ETERNAL CRIMINAL RECORD (2015).

11. Maryland v. King, 569 U.S. 435, 466, 478–82 (2013) (Scalia, J., dissenting).

not necessarily affording investigative benefit, can expose individuals to significant embarrassment.[12]

Taken together, the myriad databases, their inter-operability, and the ease with which information can be retrieved from them (by computer laptops, tablets, and handheld devices),[13] has fostered a revolution in policing akin to that of the introduction of patrol cars and two-way radios.[14] As two policing scholars recently put it, officers today engage in "database policing" in the search of "hits."[15]

Unfortunately, legal doctrine has not kept pace with these realities, with scholars and courts focusing mainly on the collection[16] and use of data.[17] This Article addresses a distinct yet equally critical important issue: police wherewithal to access databases by means of personal identifiers—a form of data matching.[18] Properly viewed, identity information is an evidentiary fruit

---

12. *See infra* text accompanying notes 271–86.

13. *See, e.g.*, David Griffith, *The Next Stage of Patrol Computers*, POLICE MAG. (Sept. 10, 2013), http://www.policemag.com/channel/technology/articles/2013/09/the-next-stage-of-patrol-computers.aspx.

14. Elizabeth E. Joh, *Policing by Numbers: Big Data and the Fourth Amendment*, 89 WASH. L. REV. 35, 37 n.21, 39 (2014). Critically important, moreover, the databases themselves often elude public attention because police departments can be reluctant to even acknowledge their existence. *See, e.g.*, Dumke & Main, *supra* note 2. And private vendors, which frequently assist in their creation, further shield public knowledge by raising intellectual property concerns. *See, e.g.*, Rebecca Wexler, *Code of Silence*, WASH. MONTHLY (June–Aug. 2017), https://washingtonmonthly.com/magazine/junejuly august-2017/code-of-silence.

15. *See* Stephen D. Mastrofski & James F. Willis, *Police Organization Continuity and Change: Into the Twenty-First Century*, 39 CRIME & JUST. 55, 88 (2010) ("Police now appear to rely more heavily on certain IT-based forms of surveillance—'database policing'—where officers use computers to 'patrol' massive data files (e.g., wanted lists) looking for 'hits' on information they possess on suspects." (citations omitted)).

16. *See, e.g.*, Fabio Arcila, Jr., *GPS Tracking Out of Fourth Amendment Dead Ends:* United States v. Jones *and the* Katz *Conundrum*, 91 N.C. L. REV. 1, 48–64 (2012) (discussing the implications and questions raised by *United States v. Jones* for the use of technological data collection methods by law enforcement); Richard A. Robertson, *The Unconstitutionality of Bulk Data Collection*, 26 B.U. PUB. INT. L.J. 151, 163–66 (2017) (arguing in favor of limits being placed on bulk data collection by governments).

17. *See, e.g.*, Emily Berman, *When Database Queries Are Fourth Amendment Searches*, 102 MINN. L. REV. 577, 585–95 (2017) (discussing the government's ability to use databases without restriction); Ric Simmons, *The Mirage of Use Restrictions*, 96 N.C. L. REV. 133 (2017) (arguing that proposed use restrictions lack sufficient justifications); Orin S. Kerr, *Use Restrictions and the Future of Surveillance Law,* BROOKINGS (April 19, 2011), https://www.brookings.edu/research/use-restrictions-and-the-future-of-surveillance-law (arguing for restrictions on the use of data collected by the government surveillance); Rebecca Lipman, Protecting Privacy with Fourth Amendment Use Restrictions 6–33 (April 9, 2017) (unpublished manuscript), *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2949293 (arguing for use restrictions on material that law enforcement lawfully collects).

18. *See* Daniel J. Steinbock, *Data Matching, Data Mining, and Due Process*, 40 GA. L. REV. 1, 3–4 (2005) (defining "data matching" as "linking individuals with data about them"); *cf.* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 551 (2005) (asserting with respect to computer data that "a search occurs when information from or about the data is exposed to possible human observation, such as when it appears on a screen, rather than when

that should be subject to suppression when it is unlawfully secured by police. Without it, information associated with an individual lies inert in government databases; with it, police can stop, arrest, search and question individuals they encounter on street patrol.

Given the voracious government appetite for information,[19] now stored and analyzed on an ever cheaper and more efficient basis,[20] and the already ample authority of police to secure identity information lawfully,[21] the stakes of regulating unlawful police access should be readily apparent. The Supreme Court's recent decision in *Utah v. Strieff*[22] provides a compelling example in this regard. After observing him leave what was believed to be a drug house, officer Douglas Fackrell unlawfully seized Edward Strieff on suspicion of being involved in illegal drug activity and demanded that he produce personal identification.[23] Upon learning his identity, Fackrell ran Strieff's name in a government database and discovered that he was the subject of "a small traffic warrant" for his arrest,[24] one of many tens of thousands arrest warrants in the database.[25] Fackrell then arrested Strieff, searched him, and discovered drug paraphernalia and a plastic baggie containing methamphetamine.[26] The Court upheld the search, concluding that the arrest warrant discovered, which "predated" and was "entirely unconnected" to the initial illegal seizure,

---

it is copied by the hard drive or processed by the computer"); Matthew Tokson, *Automation and the Fourth Amendment*, 96 IOWA L. REV. 581, 586–87 (2011) (drawing distinction between disclosure of information to automated systems and disclosure to humans and arguing that only the latter warrants Fourth Amendment protection).

19. Telling evidence of this motivational dynamic was seen in New York City, where police, before being enjoined, swabbed the inside cheeks of persons stopped (not arrested) for traffic and other minor offenses. Kevin Flynn, *Fighting Crime with Ingenuity, 007 Style; Gee-Whiz Police Gadgets Get a Trial Run in New York*, N.Y. TIMES (Mar. 7, 2000), https://www.nytimes.com/2000/03/07/nyregion/fighting-crime-with-ingenuity-007-style-gee-whiz-police-gadgets-get-trial-run.html.

20. *See* United States v. Jones, 565 U.S. 400, 415–16 (2012) (Sotomayor, J., concurring) (noting that digitization enables governments to "store . . . records and efficiently mine them for information years into the future," and avoid "the ordinary checks that constrain abusive law enforcement practices: 'limited police resources and community hostility'" (quoting Illinois v. Lidster, 540 U.S. 419, 426 (2004))).

21. *See, e.g.*, Hiibel v. Sixth Judicial Dist. Court, 542 U.S. 177, 190–91 (2004) (upholding right of police to demand personal identifying information in conjunction with a lawful stop).

22. Utah v. Strieff, 136 S. Ct. 2056 (2016).

23. Brief for Respondent at 14, Utah v. Strieff, 136 S. Ct. 2056 (No. 14-1373), 2016 WL 1254378, at *14 (citing record evidence that officer "admitted . . . he 'had no reason to stop'" Strieff and that he demanded "identification because he wanted 'to know who I'm talking to'" (quoting Officer Fackrell)).

24. State v. Strieff, 357 P.3d 532, 536 (Utah 2015), *rev'd*, Utah v. Strieff, 136 S. Ct. 2056 (2016). The record was unclear on the precise basis for the warrant, which Justice Sotomayor in dissent described as concerning "an unpaid parking ticket" and "a 'small traffic warrant.'" *Id.* at 2064–65 (Sotomayor, J., dissenting).

25. *Id.* at 2066.

26. *Id.* at 2060 (majority opinion).

was an intervening circumstance that attenuated the evidence seized from the unlawful seizure.[27]

To seasoned modern-day Court watchers, accustomed to its disdain for the exclusionary rule,[28] *Strieff* perhaps came as no surprise.[29] On the streets, however, there is no mistaking that *Strieff* will have major significance: police can now unlawfully seize individuals and demand personal identity information, providing entre to a vast realm of database information. Moreover, although *Strieff* involved the unlawful seizure of a pedestrian,[30] its logic extends to vehicle stops by police,[31] which number in the many millions annually.[32] For officers engaged in what Justice Robert Jackson famously termed the "competitive enterprise of ferreting out crime,"[33] the benefits are as broad as the expanse of databases on which they have come to rely, which is very broad indeed.

The discussion proceeds as follows. Part II surveys the increasingly important role identity-related data has come to play in policing and then focuses on two judicial doctrines that allow police to use unlawfully secured identity evidence and the information that flows from it. The first, attenuation doctrine, relied upon most recently by the Supreme Court in *Strieff*, allows evidence to be used in a prosecution even when it is unlawfully secured by police, based on the rationale that the causal connection between the misconduct and the evidence is attenuated.

Strieff, as will be discussed, is a poorly reasoned opinion that significantly increases police authority to secure identity information. The five-member majority (and indeed the dissenting Justices), however, asked the wrong question: it was not whether the discovered arrest warrant was causally linked to the illegal stop; it was not, as it clearly "predated" the unlawful seizure. What the officer lacked was a way to access the arrest warrant in the government database, which he accomplished only by means of unlawfully demanding

---

27. *Id.* at 2062.

28. *See, e.g.*, Jennifer E. Laurin, *Trawling for* Herring: *Lessons in Doctrinal Borrowing and Convergence*, 111 COLUM. L. REV. 670, 724–39 (2011); Tracey Maclin & Jennifer Rader, *No More Chipping Away: The Roberts Court Uses an Axe to Take Out the Fourth Amendment Exclusionary Rule*, 81 MISS. L.J. 1183, 1184–201 (2012).

29. *See, e.g.*, Orin Kerr, *Opinion Analysis: The Exclusionary Rule Is Weakened but It Still Lives*, SCOTUSBLOG (June 20, 2016, 9:35 PM), http://www.scotusblog.com/2016/06/opinion-analysis-the-exclusionary-rule-is-weakened-but-it-still-lives (asserting "that the [*Strieff*] majority opinion did not overturn or substantially revise" prior doctrine).

30. *Strieff*, 136 S. Ct. at 2063–65.

31. *See, e.g.*, United States v. Patrick, 842 F.3d 540, 542 (7th Cir. 2016) ("*Strieff* tells us that, if the police had stopped [defendant's] car for no reason at all and learned only later that he was a wanted man, the gun would have been admissible in evidence.").

32. *See Traffic Stops*, BUREAU JUST. STAT., http://www.bjs.gov/index.cfm?ty=tp&tid=702 (last visited Oct. 21, 2018). The stops themselves are often pretextual in nature, serving as bases to potentially secure information regarding more serious criminal activity (frequently illegal drugs). *See* Wayne A. Logan, Erie *and Federal Criminal Courts*, 63 VAND. L. REV. 1241, 1248 n.26 (2010).

33. Johnson v. United States, 333 U.S. 10, 14 (1948).

Strieff's identification. The "fruit" of the illegal seizure, in other words, was not the arrest warrant—it was the unlawfully demanded identifier that linked Strieff to the database and the arrest warrant.

The second doctrine, what will be called the "identity exception," provides that personal identity information is never subject to exclusion, nor is the incriminating database information that it allows police to access. It too rests on dubious jurisprudential grounds and incentivizes police to unlawfully seize individuals, demand identity information, and reap database investigative rewards.

Part III examines the practical significance of expanding police authority to unlawfully access government databases. It does so by surveying the vast array of information now available to police, including that regarding stops, arrests and convictions; biometric identification data; evidence unlawfully secured but retained by police; and even personally sensitive information (e.g., history of drug use or depression). The data, which can be inaccurate or reflective of racialized policing practices, can have major investigative value for police, or at a minimum reveal embarrassing facts about individuals targeted.

The *Strieff* dissents properly voiced concern over police undertaking "fishing expeditions" to discover arrest warrants in databases, allowing them to arrest, search, and secure evidence for other, unrelated prosecutions (like the drugs found on Strieff).[34] The incentive structure operates similarly to other database information accessible to police. Part III concludes with a discussion of the very significant consequences of expanded police access to database information, ranging from the heightened likelihood of factually innocent individuals being unlawfully seized by police to damaging public willingness to engage in civic life.

Part IV sketches a path forward. It does so by first clearing away some basic doctrinal confusion that has contributed to the judicial failure to limit police authority to access database information. In particular, courts, including the Supreme Court in *Strieff*, have wrongly attached importance to the fact that the information unlawfully accessed by police pre-exists the challenged police wrongdoing, relying on doctrine that is a poor fit for the technological realities of modern day policing. With Fourth Amendment doctrine, rather than framing analysis in attenuation doctrine, scenarios such as in *Strieff* should be conceived as identity-data seizures. Officer Fackrell not only unlawfully seized Strieff; he also unlawfully demanded and secured his identification information, resulting in an arrest and search revealing contraband. Search and seizure doctrine must take account of the critical practical significance of unlawful personal identity seizures by police. Alternatively, unlawfully compelling identity information can be seen as implicating the Fifth Amendment privilege against compelled self-

34. *Strieff*, 136 S. Ct. at 2064–65 (Sotomayor, J., dissenting); *id.* at 2071 (Kagan, J., dissenting).

incrimination. As the Court acknowledged in *Hiibel v. Sixth Judicial District of Nevada*, compelled identity information can have incriminating effect when it is used to access a database containing incriminating information.[35] The same concern can arise when police access other incriminating data contained in databases. The Article closes with discussion of the prospects for a legislatively imposed limit on police authority, which, despite its considerable appeal, would not likely come to pass for political process and public choice reasons well known to criminal justice policy-making.

II. POLICE AUTHORITY TO ACCESS DATABASES

Law enforcement has long collected information on individuals thought to present criminal risk.[36] Whereas early on such knowledge was reposed in individual officers, with a few revered for their remarkable prowess for recognizing human faces,[37] by the mid-19th century America had become increasingly urbanized and populous, straining the identification capacity of police.[38] The advent of photography allowed for the capturing and storage of facial images,[39] a critically important advance soon complemented by other identification methods, including anthropometry (involving the measurement of body parts such as the ears and heads and storage of such information on index cards).[40] By the early 20th century fingerprints became the dominant identification tool.[41]

It did not take long, however, for the practice to generate concern. In 1916, for instance, police were publicly criticized for collecting fingerprints

---

35. *See* Hiibel v. Sixth Judicial Dist. Court, 542 U.S. 177, 191 (2004) ("[F]urnishing identity [can] . . . give[] police a link in the chain of evidence needed to convict the individual of a separate offense.").

36. For a fuller historical survey of the importance to police of personal identity-related information in monitoring perceived risk, see Wayne A. Logan, *Policing Identity*, 92 B.U. L. REV. 1561, 1564–75 (2012).

37. *See, e.g.*, HOWARD O. SPROGLE, THE PHILADELPHIA POLICE, PAST AND PRESENT 273, 653 (1971) (noting that "[a] good detective's memory is a rogues' gallery in itself" and describing one detective as having "a wonderful memory of faces and names").

38. *See* GUSTAVE DE BEAUMONT & ALEXIS DE TOCQUEVILLE, ON THE PENITENTIARY SYSTEM IN THE UNITED STATES AND ITS APPLICATION IN FRANCE 101 (Francis Lieber trans., S. Ill. Univ. Press 1964) (1833) (observing that in America "[n]othing is easier than to pass from one state to another, and it is in the criminal's interest to do so").

39. *See* JAMES F. RICHARDSON, THE NEW YORK POLICE: COLONIAL TIMES TO 1901, at 122 (1970) (noting the first use of a "rogues gallery" in 1857); *see also* SPROGLE, *supra* note 37, at 265–66 (describing use of five-foot tall cabinet containing racks of photographs with an index allowing access to information regarding prior criminal activity and other identifying information).

40. *See* RONALD R. THOMAS, DETECTIVE FICTION AND THE RISE OF FORENSIC SCIENCE 223 (1999) (noting that anthropometry was premised on the idea "that the body betrays the truth about the criminal in the form of an automatic anatomical writing that is legible to the eyes of the trained expert").

41. *See generally* SIMON A. COLE, SUSPECT IDENTITIES: A HISTORY OF FINGERPRINTING AND CRIMINAL IDENTIFICATION (2001) (detailing the global history of fingerprinting as a method of identifying criminals).

from individuals arrested for minor offenses because they would be "branded as . . . criminal[s]."[42] Courts were similarly concerned,[43] with Berkeley Law Professor A.M. Kidd observing that "[t]hey d[id] not sanction the common practice of 'mugging' every suspect whose picture and measurements the police would like to have. Nor [did the courts] sustain the right to retain the prints and measurements after acquittal."[44] Surveying the caselaw, Professor Kidd noted that a handful of decisions adopted a more generous stance,[45] but emphasized "that [even such] cases [went] no further than to permit the taking of photographs and measurements of persons suspected of serious offenses, for the purpose of identification."[46]

Early courts also made clear their concern over public display of arrestees' photos in police station "rogues galleries."[47] It was not uncommon for individuals to win injunctive relief allowing for the destruction or return of photographic plates in the possession of police.[48] Likewise, in an important early decision, *United States v. Kelly*,[49] the Second Circuit upheld the right of police to secure fingerprints in order to "ascertain[] whether a defendant has been previously convicted, so that the prior conviction can be pleaded as required in . . . the National Prohibition Act."[50] In so holding, however, the court emphasized that the long-term negative effect of the policy was limited

42. *Id.* at 157; *see also* John Elfreth Watkins, *"Mugging" Innocent Persons Under Arrest: Lights and Shadows of a System Whose Abuse Has Shaken New York's Police from Top to Bottom*, SUNDAY OREGONIAN, July 25, 1909, at 4 (reporting instances of perceived police abuses).

43. *See, e.g.*, People v. Hevern, 215 N.Y.S. 412, 418 (Magis. Ct. 1926) (deeming "compulsory finger printing before conviction . . . an unlawful encroachment upon person, in violation of the state and federal Constitutions"); *see also* Joseph M. Deuel, *What There Is in Finger-Prints*, *in* FINGER-PRINTS 3, 10 (1917) (relaying from author's experience as a New York City Magistrate that "[t]here must be an arrest . . . and a plea of guilty or a conviction on competent evidence before there can be finger-printing; there can be none on an acquittal"); *Finger-Printing*, EVENING WORLD DAILY MAG., Dec. 19, 1916, at 16 (lauding refusal of several magistrates to engage in "routine" fingerprinting of persons arrested for petty offenses, condemning the collection "preposterous, barbarous").

44. A.M. Kidd, *The Right to Take Fingerprints, Measurements and Photographs*, 8 CALIF. L. REV. 25, 32 (1919).

45. *Id.* at 30–32 (citing Mabry v. Kettering, 122 S.W. 115 (Ark. 1909), Shaffer v. United States, 24 App. D.C. 417 (D.C. Cir. 1904), and Downs v. Swann, 73 A. 653 (Md. 1909)).

46. *Id.* at 32.

47. *See, e.g.*, *Downs*, 73 A. at 656 (refusing "to countenance the placing in the rogues' gallery of the photograph of any person, not a habitual criminal, who has been arrested, but not convicted, on a criminal charge, or the publication under those circumstances of his Bertillon [anthropometric] record"); *Brokaw's Caretaker Held on Two Charges*, N.Y. TIMES, Mar. 13, 1905, at 5 (quoting magistrate: "'I do not approve of photographing a man for the Rogues' Gallery until after he is convicted,' . . . . 'I have always been opposed to the idea. Once a man's picture is in the Rogues' Gallery it is difficult for him to get it out.'").

48. *See, e.g.*, Itzkovitch v. Whitaker, 42 So. 228, 229 (La. 1906) (ordering return of photo plate and destruction of fingerprints and measurements and stating that continued exhibition would be an unjust "permanent proof of dishonesty").

49. United States v. Kelly, 55 F.2d 67 (2d Cir. 1932).

50. *Id.* at 70.

because identification data had to be destroyed or surrendered to the individual in the event the charge was dismissed or there was an acquittal.[51]

The *Kelly* court's insistence that identity evidence be destroyed absent conviction now seems a quaint reminder of a bygone past. Today, as will be discussed in Part III, a vast array of identity-related evidence is freely collected by police and stored in government databases, much of it concerning individuals not convicted of a crime.[52] At the same time, police today enjoy unprecedented technological wherewithal to quickly and readily access databases by means of laptops and handheld devices.[53]

The importance of police knowledge of individual identity has grown alongside these technological advances. Police can secure knowledge of identity in any number of lawful ways. They can of course recognize an individual[54] or request disclosure of a name or other identifying data such as DNA or a fingerprint, even by means of trickery or stealth.[55]

This Part focuses on police unlawful acquisition of identity information and its role in accessing database information. It does so by examining two exceptions to the Fourth Amendment exclusionary rule: attenuation doctrine and the "identity exception."

A. ATTENUATION DOCTRINE

After recognizing the exclusionary rule, first in 1914 for federal criminal trials,[56] and 1961 for state criminal trials,[57] the Supreme Court has limited its application in several critically important ways.[58] One exception concerns

---

51. *Id.*

52. *See* People v. McInnis, 494 P.2d 690, 692 (Cal. 1972) (noting over 40 years ago that "thousands of persons ultimately found to be entirely innocent undoubtedly have their photographs, as well as fingerprints, on record with law enforcement agencies").

53. For early discussion of this evolution and concerns raised, see Kenneth L. Karst, *"The Files": Legal Controls Over the Accuracy and Accessibility of Stored Personal Data*, 31 LAW & CONTEMP. PROBS. 342, 365–66 (1966); Project, *The Computerization of Government Files: What Impact on the Individual?*, 15 UCLA L. REV. 1371, 1411–25 (1968); Comment, *Retention and Dissemination of Arrest Records: Judicial Response*, 38 U. CHI. L. REV. 850, 853 (1971).

54. Scotland Yard in England now boasts a cadre of "super-recognizers" who scan visages captured on film provided by the many video cameras now in use. *See* Patrick Radden Keefe, *The Detectives Who Never Forget a Face*, NEW YORKER (Aug. 22, 2016), http://www.newyorker.com/magazine/2016/08/22/londons-super-recognizer-police-force.

55. *See* Elizabeth E. Joh, *Bait, Mask, and Ruse: Technology and Police Deception*, 128 HARV. L. REV. F. 246, 247–48 (2015).

56. Weeks v. United States, 232 U.S. 383, 398 (1914), *overruled on other grounds by* Mapp v. Ohio, 367 U.S. 643 (1961).

57. *Mapp*, 367 U.S. at 659–60.

58. *See* 1 JOSHUA DRESSLER & ALAN C. MICHAELS, UNDERSTANDING CRIMINAL PROCEDURE: INVESTIGATION 375–80 (6th ed. 2013) (noting and explaining the (1) independent source doctrine; (2) inevitable discovery rule; and (3) attenuated connection doctrine). The independent source doctrine provides that evidence secured as the result of police misconduct can be admissible if it is later obtained lawfully on an independent basis. *See* Murray v. United States, 487 U.S. 533, 537 (1988). The inevitable discovery doctrine provides that illegally secured

situations where the police engage in misconduct, for instance an illegal arrest, and thereby secure evidence that serves as a basis for criminal prosecution. Typically, the exclusionary rule would apply in such a situation, barring both evidence that was directly obtained by the illegality (e.g., drugs discovered in a search) and "fruits" indirectly leading to a later intrusion by police (e.g., papers discovered in the initial search providing knowledge for a later search).[59]

The attenuation doctrine, however, allows such information to be used under certain circumstances. Even though the information would not have been discovered "but for" the illegality, attenuation permits its use if the connection between the misconduct and its discovery is thought sufficiently weak as to remove the taint of the initial illegality.[60]

The exception originated in 1939 in *Nardone v. United States*,[61] but was articulated more fully almost a quarter century later in *Wong Sun v. United States*.[62] In *Wong Sun*, the Court held that a confession provided by a wrongfully arrested individual was not subject to suppression because "the connection between the arrest and the statement had 'become so attenuated as to dissipate the taint.'"[63] The confession was attenuated from the illegal arrest, the Court reasoned, because after the arrest Wong Sun was released on his own recognizance and, as "an intervening independent act of free will,"[64] a few days later voluntarily returned to the police station and provided the statement.[65] The central question, the Court wrote, was "whether, granting establishment of the primary illegality, the evidence [secured] . . . has been come at by exploitation of that illegality or instead by means sufficiently distinguishable to be purged of the primary taint."[66]

---

evidence can be admissible if it can be established that the evidence would have been inevitably discovered in the absence of the police misconduct. *See* Nix v. Williams, 467 U.S. 431, 444 (1984). The "good faith" exception, triggered when police violate the law but do so in a manner that is deemed objectively constitutionally reasonable, is yet another key exception to the exclusionary rule. *See* 1 DRESSLER & MICHAELS, *supra*, at 363–73.

59. *See* Segura v. United States, 468 U.S. 796, 804 (1984) ("[T]he exclusionary rule reaches not only primary evidence obtained as a direct result of an illegal search or seizure, but also evidence later discovered and found to be derivative of an illegality or 'fruit of the poisonous tree.'" (citation omitted)).

60. 1 DRESSLER & MICHAELS, *supra* note 58, at 379.

61. Nardone v. United States, 308 U.S. 338, 341 (1939) ("Sophisticated argument may prove a causal connection between information obtained through illicit wire-tapping and the Government's proof. As a matter of good sense, however, such connection may have become so attenuated as to dissipate the taint.").

62. Wong Sun v. United States, 371 U.S. 471, 491 (1963).

63. *Id.* (quoting *Nardone*, 308 U.S. at 341).

64. *Id.* at 486 (quoting the Government); *see also id.* at 491 (finding that Wong Sun's release from police custody and voluntary return to the police station a few days later to give a statement qualified as attenuation).

65. *Id.* at 491.

66. *Id.* at 488 (quoting JOHN MACARTHUR MAGUIRE, EVIDENCE OF GUILT: RESTRICTIONS UPON ITS DISCOVERY OR COMPULSORY DISCLOSURE 221 (1959)).

Brown v. Illinois[67] was the Court's next, more complete discussion of attenuation. In *Brown*, the Court concluded that police provision of Miranda warnings did not purge the taint of an earlier illegal arrest, requiring that defendant's confession be suppressed.[68] The Court stated that allowing provision of Miranda rights alone to purge the taint of an illegal arrest would "substantially dilute[]" the exclusionary rule's protection of Fourth Amendment rights, signaling to police that they could illegally arrest individuals confident in the knowledge that they could use any incriminating statements secured.[69] The Court identified several factors to consider when evaluating whether the attenuation exception should apply: (1) the temporal proximity between the police wrongdoing and the evidence secured; (2) "the presence of intervening circumstances" (such as provision of Miranda warnings); and (3) "particularly, the purpose and flagrancy of the official misconduct."[70]

Utah v. Strieff is the Court's most recent application of the attenuation doctrine.[71] In *Strieff*, the Court addressed whether police discovery of an arrest warrant in a government database, leading to an arrest and discovery of contraband, purged the taint of the initial unlawful seizure that led to the arrest and search.[72] Siding with the minority position of federal circuits addressing the issue,[73] the Court held that "discovery of a valid, pre-existing, and untainted arrest warrant" was an intervening event that attenuated the police misconduct leading to its discovery.[74] In so doing, the majority rejected the unanimous view of the Utah Supreme Court that the Court's prior case law only considered "a voluntary act of a defendant's free will (as in a confession or consent to search)" as a sufficient intervening circumstance.[75] Applying the three *Brown* factors, the majority concluded that the close temporal proximity between the unlawful seizure of Strieff and demand of his identification weighed in favor of application of the exclusionary rule.[76]

The second *Brown* factor, the presence of an intervening circumstance, however, "strongly favor[ed] the State."[77] The majority's analysis relied in

67. Brown v. Illinois, 422 U.S. 590 (1975).

68. *Id.* at 605.

69. *Id.* at 602.

70. *Id.* at 603–04.

71. Utah v. Strieff, 136 S. Ct. 2056 (2016).

72. *Id.* at 2059.

73. *See* Merry C. Johnson, Comment, *Discovering Arrest Warrants During Illegal Traffic Stops: The Lower Courts' Wrong Turn in the Exclusionary Rule Attenuation Analysis*, 85 MISS. L.J. 225, 237–39 (2016) (noting that the Sixth, Ninth and Tenth Circuits held that the discovery of an arrest warrant did not qualify as an intervening act sufficient to purge the taint of an illegal seizure, while the Seventh and Eighth Circuit adopted the contrary view).

74. *Strieff*, 136 S. Ct. at 2061, 2063.

75. *Id.* at 2060 (quoting State v. Strieff, 357 P.3d 532, 536 (Utah 2015)).

76. *Id.* at 2061–63.

77. *Id.* at 2062.

significant part on *Segura v. United States*,[78] which was based on another exclusionary rule exception: the independent source doctrine, which allows admission of evidence if it was actually secured on a lawful basis independent of police wrongdoing.[79] In *Segura*, police unlawfully entered a residence and discovered evidence of illegal drug activity, yet the search warrant later obtained was based on information "wholly unconnected with the [arguably illegal] entry and was known to the agents well before the initial entry."[80] The *Strieff* majority acknowledged that *Segura* applied the independent source exception, yet added that "the *Segura* Court suggested that the existence of a valid warrant favors finding that the connection between unlawful conduct and the discovery of evidence is 'sufficiently attenuated to dissipate the taint.' That principle applies here."[81] This was because the warrant

> predated [the officer's] investigation, and it was entirely unconnected with the stop. And once [the officer] discovered the warrant, he had an obligation to arrest Strieff. . . . [The officer's] arrest of Strieff thus was a ministerial act that was independently compelled by the pre-existing warrant. And once [the officer] was authorized to arrest Strieff, it was undisputedly lawful to search Strieff as an incident of his arrest . . . .[82]

Finally, the majority concluded that "the third [*Brown*] factor, 'the purpose and flagrancy of the official misconduct,' also strongly favor[ed] the State."[83] According to the majority, the officer was "at most negligent" when he unlawfully stopped Strieff; furthermore, his "decision to run the warrant check was a 'negligibly burdensome precautio[n]' for officer safety."[84]

The majority opinion, authored by Justice Thomas, was met by two vigorous dissents, by Justices Sotomayor and Kagan, with Justice Ginsburg joining Kagan's dissent and most but not of all of Sotomayor's dissent.[85] Justice Sotomayor at the outset warned of the significant practical consequences flowing from the majority's refusal to apply the exclusionary rule:

> Do not be soothed by the [majority's] technical language: This case allows police to stop you on the street, demand your identification,

78. *Id.* at 2062 (citing Segura v. United States, 468 U.S. 796, 799–801, 814–15 (1984)).

79. *See* 1 DRESSLER & MICHAELS, *supra* note 58, at 375–78.

80. *Strieff*, 136 S. Ct. at 2062 (alteration in original) (quoting *Segura*, 468 U.S. at 814).

81. *Id.* (citation omitted) (quoting *Segura*, 468 U.S. at 815).

82. *Id.* at 2062–63.

83. *Id.* at 2063 (citation omitted).

84. *Id.* (citation omitted) (quoting Rodriguez v. United States, 135 S. Ct. 1609, 1616 (2015)).

85. *Id.* at 2059; *id.* at 2064 (Sotomayor, J., dissenting); *id.* at 2071 (Kagan, J., dissenting). Due to Justice Scalia's death, the Court had only eight members at the time *Strieff* was decided (accounting for the 5-3 vote). *See* Adam Liptak, *Supreme Court Says Police May Use Evidence Found After Illegal Stops*, N.Y. TIMES (June 20, 2016), https://www.nytimes.com/2016/06/21/us/supreme-court-says-police-may-use-evidence-found-after-illegal-stops.html.

> and check it for outstanding traffic warrants—even if you are doing nothing wrong. If the officer discovers a warrant for a fine you forgot to pay, courts will now excuse his illegal stop and will admit into evidence anything he happens to find by searching you after arresting you on the warrant.[86]

In an expansive opinion, citing sources such as W.E.B. Du Bois, James Baldwin, and Ta-Nehisi Coates, Sotomayor first questioned the majority's conclusion that the officer did not find drugs on Strieff as a result of exploiting his illegal seizure.[87] "The officer did not ask Strieff to volunteer his name only to find out, days later, that Strieff had a warrant against him. [Officer Fackrell] illegally stopped Strieff and immediately ran a warrant check."[88] She added that finding the outstanding arrest warrant for Strieff "was not some intervening surprise that he could not have anticipated," given that Utah had over 180,000 outstanding misdemeanor arrest warrants in its database, and a "'backlog of arrest warrants' so large that it faced the 'potential for civil liability.'"[89] Accordingly, "[t]he warrant check . . . was not an 'intervening circumstance' separating the stop from the search for drugs. It was part and parcel of the officer's illegal 'expedition for evidence in the hope that something might turn up.'"[90]

Justice Sotomayor also questioned the majority's reliance on *Segura v. United States*, which she asserted was used in such a way that "'suggests[s]' that a valid warrant will clean up whatever illegal conduct uncovered it."[91] She noted that in *Segura* the illegal home entry by police "had nothing to do with [the] . . . search warrant" for the home that was secured[92]—i.e., the support for the search warrant was independent of the information learned as a result of the illegal entry. "*Segura* would be similar," Sotomayor wrote, "only if the agents [there had] used information they illegally obtained from the apartment to procure a search warrant or discover an arrest warrant."[93] In *Strieff*, on the other hand, the officer's illegal seizure "was essential to his discovery of an arrest warrant."[94]

In the last part of her opinion (which Justice Ginsburg did not join), Justice Sotomayor highlighted the many negative consequences of being seized by police, lawfully or unlawfully, including public embarrassment, enduring the privacy invasion of searches, and the serious life-long burdens

86. *Strieff*, 136 S. Ct. at 2064 (Sotomayor, J., dissenting).
87. *Id.* at 2070.
88. *Id.* at 2066.
89. *Id.* (citations omitted).
90. *Id.* (quoting Brown v. Illinois, 422 U.S. 590, 603–05 (1975)).
91. *Id.* at 2067 (alteration in original) (quoting *id.* at 2062–63 (majority opinion)).
92. *Id.*
93. *Id.*
94. *Id.*

of having an arrest record.[95] Furthermore, noting that Strieff himself was white "shows that anyone's dignity can be violated in this manner. But it is no secret that people of color are disproportionate victims of this type of scrutiny."[96] In conclusion, Justice Sotomayor wrote:

> [T]his case tells everyone, white and black, guilty and innocent, that an officer can verify your legal status at any time. It says that your body is subject to invasion while courts excuse the violation of your rights. It implies that you are not a citizen of a democracy but the subject of a carceral state, just waiting to be cataloged.[97]

Justice Kagan began her dissent by noting that if drugs were found on Strieff, after his initial illegal seizure, the drugs would be suppressed, and contended that the facts in Strieff's case should not dictate a different result.[98] Applying the three *Brown* factors, she agreed that because the officer's discovery of drugs on Strieff occurred shortly after the illegal seizure, "the State . . . takes strike one."[99] She strongly disagreed, however, with the majority's conclusion that the officer's misconduct involved "a couple of innocent 'mistakes.' . . . [F]ar from a Barney Fife-type mishap, [the officer's] seizure of Strieff was a calculated decision, taken with so little justification that the State has never tried to defend its legality."[100] Like Justice Sotomayor, Justice Kagan criticized the majority's reliance upon *Segura*,[101] and asserted that a circumstance is "intervening" for attenuation purposes "only when it is unforeseeable," and discovery of an outstanding arrest warrant "was an eminently foreseeable consequence."[102]

Indeed, Justice Kagan contended, it was standard procedure in the officer's department to "stop, ask for identification, run a check—[all] partly designed to find outstanding warrants. And find them they will, given the staggering number of such warrants on the books."[103] According to Justice Kagan:

> [O]utstanding warrants do not appear as bolts from the blue. They are the run-of-the-mill results of police stops—what officers look for when they run a routine check of a person's identification and what

95. *Id.* at 2069–70.

96. *Id.* at 2070 (citation omitted).

97. *Id.* at 2070–71.

98. *Id.* at 2071 (Kagan, J., dissenting) (asserting that the "added wrinkle [of the discovered warrant] makes no difference under the Constitution").

99. *Id.* at 2072.

100. *Id.* (quoting *id.* at 2063 (majority opinion)).

101. *See id.* at 2073 n.2 (asserting that *Segura* "lacks any relevance" to the situation in *Strieff*, one "when an unconstitutional act in fact leads to a warrant which then leads to evidence").

102. *Id.* at 2073.

103. *Id.*

> they know will turn up with fair regularity. In short, they are nothing like what intervening circumstances are supposed to be.[104]

In closing, Justice Kagan wrote that the majority's opinion

> creates unfortunate incentives for the police—indeed, practically invites them to do what [the officer] did here. . . . So long as the target [of an illegal seizure] is one of the many millions of people in this country with an outstanding arrest warrant, anything the officer finds in a search is fair game for use in a criminal prosecution. . . . From here on, [the officer] sees potential advantage in stopping individuals without reasonable suspicion—exactly the temptation the exclusionary rule is supposed to remove.[105]

For reasons identified in the dissents, *Strieff* lacks doctrinal merit and creates significant incentives for police to unlawfully seize individuals, demand identification, and run a warrant check.[106] While Justice Sotomayor's stirring dissent with its literary flourishes will long be noted,[107] *Strieff* will turn out to be significant for far more than this alone. This is because of the Court's willingness to regard as an "intervening circumstance" the "pre-existing [arrest] warrant," and its failure to appreciate the constitutional significance of the officer's unlawful demand of Strieff's identification (separate from his unlawful seizure), which allowed access to the database containing the warrant.[108]

Conceiving of the arrest warrant as the Court did was accurate in one sense. As a temporal matter, it surely did pre-exist Strieff's unlawful seizure, and it was based on conduct unrelated to the reason he was seized (his previous failure to appear in court to resolve a "small traffic warrant").[109] The crucial analytic point elided by the *Strieff* majority, however, was how police accessed the arrest warrant: by means of his unlawfully secured identity information. When this is the analytic focus, the majority's invocation of *Segura* becomes even more inapt. As suggested by Justice Sotomayor,[110] the decision would only be analogous if police learned that Segura resided in the apartment by means of unlawfully seizing him and demanding his name. In

104. *Id.*

105. *Id.* at 2073–74.

106. As Orin Kerr has observed, "[i]f there's no warrant out for his arrest, you can let him go and he's extremely unlikely to sue. If there is a warrant, you can arrest him, search him incident to arrest, and question him later . . . . If in doubt, make the stop." Kerr, *supra* note 29.

107. *See id.* (asserting that "I suspect that this case will become most known for Part IV of Justice Sonia Sotomayor's dissent. Citing sources ranging from Ta-Nehisi Coates to Michelle Alexander, Sotomayor gives voice to the anger and frustration of social movements such as Black Lives Matter.").

108. *Strieff*, 136 S. Ct. at 2062–63.

109. *Id.* at 2065 (Sotomayor, J., dissenting) (quoting a trial document).

110. *See id.* at 2067 ("*Segura* would be similar only if the agents [there had] used information they illegally obtained from the apartment to procure a search warrant or discover an arrest warrant.").

other words, the critical factor in *Strieff* was the unlawful demand of identity, which linked Strieff to the arrest warrant database. It was not the pre-existing warrant itself. And because Strieff's name was secured by "exploiting" his illegal seizure[111] for investigative purposes,[112] access to the arrest warrant, and the arrest and search revealing contraband, were invalid.

In short, the *Strieff* majority (and indeed the two dissents) asked the wrong question: it was not whether the discovered arrest warrant was causally linked to the illegal stop; it clearly was not. If the facts were otherwise—if Officer Fackrell knew Strieff had a warrant out on him, and knew his identity, or lawfully requested his identification, the ensuing arrest and search clearly would be lawful. What the officer lacked was a way to access the database, which he accomplished only by means of illegally seizing Strieff and demanding his identification. The "fruit" of the illegal seizure, again, was not the arrest warrant—it was the unlawfully secured personal identifier that linked Strieff to the database and the arrest warrant.

After *Strieff*, so long as the basis for a lawful seizure (or search) "pre-exist[s]" and is "independent" of police wrongdoing, it is fair game for police to access in a database, even when they do so as a result of an illegally obtained identifier.[113] By wrongly infusing attenuation with independent source doctrine, and ignoring the key role played by identity in police street craft, the *Strieff* majority constitutionally disembodied database information from any causal role in exclusionary rule analysis.[114]

B. THE IDENTITY EXCEPTION

The importance to police of identity information, and its role in accessing database information, is not lost on the courts. Indeed, in *Brown v. Texas* the Supreme Court expressly prohibited police from unlawfully seizing an individual simply "to ascertain . . . identity,"[115] expressing concern over "the risk of arbitrary and abusive police practices."[116] Twenty-five years later,

111. *See* Wong Sun v. United States, 371 U.S. 471, 488 (1963) (describing the primary inquiry as whether the evidence in question was secured through the "exploitation of [an] illegality or instead by means sufficiently distinguishable to be purged of the primary taint" (quoting MAGUIRE, *supra* note 66, at 221)).

112. The officer admitted that the purpose of the seizure was investigatory. *See Strieff*, 136 S. Ct. at 2072 (Kagan, J., dissenting). Investigative motivation was deemed indicative of purposefulness in *Brown v. Illinois*. Brown v. Illinois, 422 U.S. 590, 605 (1975) (finding purposefulness when officers admitted "that the purpose of their action was 'for investigation' or for 'questioning'").

113. *Strieff*, 136 S. Ct. at 2062–63; *see also id.* at 2063 ("[T]he unlawful stop was sufficiently attenuated by the pre-existing arrest warrant. . . . The outstanding arrest warrant for Strieff's arrest is a critical intervening circumstance that is wholly independent of the illegal stop.").

114. *See id.* at 2067 (Sotomayor, J., dissenting) (noting that "[t]he mere existence of a warrant not only gives an officer legal cause to arrest and search a person, it also forgives an officer who, with no knowledge of the warrant at all, unlawfully stops that person on a whim or a hunch").

115. Brown v. Texas, 443 U.S. 47, 52 (1979).

116. *Id.*

in *Hiibel v. Sixth Judicial District Court of Nevada*, a case involving a suspect lawfully seized by police, the Court acknowledged "that furnishing identity [can] . . . give[] police a link in the chain of evidence needed to convict the individual of a separate offense."[117]

Despite *Brown* and *Hiibel*, the parameters of police authority to unlawfully seize individuals, demand identity information, and use it for investigative purposes remain somewhat unclear. In significant part the confusion can be traced to the Supreme Court's 1984 decision in *INS v. Lopez-Mendoza*.[118] The case concerned the illegal arrest of two Mexican nationals, including one, Lopez-Mendoza, who objected to being summoned to a deportation hearing based on identity information surrendered to agents when he was illegally arrested.[119] The other individual, Sandoval-Sanchez, sought to have identity-related evidence linking him to his immigration record suppressed.[120] The Court, by a five-four vote, rejected both claims.[121]

At the outset of its opinion, seemingly directing itself to *Lopez-Mendoza*'s jurisdictional claim, the majority wrote that "[t]he 'body' or identity of a defendant or a respondent in a criminal or civil proceeding is never itself suppressible as a fruit of an unlawful arrest, even if it is conceded that an unlawful arrest, search, or interrogation occurred."[122] Turning to Sandoval-Sanchez's "more substantial claim," challenging not his physical presence in court but rather identity evidence offered at the hearing, the majority cast the issue in terms of whether the exclusionary rule applied to deportation proceedings.[123]

Even though deportation proceedings have long been exempt from application of the exclusionary rule, the majority analyzed whether the rule should apply, weighing the benefits of exclusion—especially deterrence of police misconduct—against the costs of excluding probative evidence.[124] According to the majority, any possible deterrent effect was reduced by several factors, including that proof of alienage could "sometimes be [proven] using

117. Hiibel v. Sixth Judicial Dist. Court, 542 U.S. 177, 191 (2004); *see also id.* at 196 (Stevens, J., dissenting) ("[A] name can provide the key to a broad array of information about the person, particularly in the hands of a police officer with access to a range of law enforcement databases. And that information, in turn, can be tremendously useful in a criminal prosecution."). Prior to *Hiibel*, the right of police to demand identity information from a lawfully detained person was less than certain. *See, e.g.*, Berkemer v. McCarty, 468 U.S. 420, 439 (1984) (stating in dictum that a suspect detained during a lawful *Terry* stop "is not obliged to respond" to questions); Terry v. Ohio, 392 U.S. 1, 34 (1968) (White, J., concurring) (stating that a lawfully detained suspect can be questioned but "is not obliged to answer, answers may not be compelled, and refusal to answer furnishes no basis for arrest").

118. I.N.S. v. Lopez-Mendoza, 468 U.S. 1032 (1984).

119. *Id.* at 1034.

120. *Id.* at 1037.

121. *Id.* at 1050–51.

122. *Id.* at 1039.

123. *Id.* at 1040–41.

124. *Id.* at 1041–50.

evidence gathered independently of, or sufficiently attenuated from, the original arrest";[125] that internal immigration agency rules had provisions deterring Fourth Amendment violations by agents;[126] and that declaratory relief was available for agency-wide abuse.[127]

The societal costs of exclusion, on the other hand, were "both unusual and significant."[128] Not only are exclusionary rule proceedings inconsistent with the "deliberately . . . streamlined" immigration system,[129] but immigration violations themselves present special concern.[130] Suppression of evidence resulting in

> [Sandoval-Sanchez's] release would clearly frustrate the express public policy against an alien's unregistered presence in this country. . . . The constable's blunder may allow the criminal to go free, but we have never suggested that it allows the criminal to continue in the commission of an ongoing crime. When the crime in question involves unlawful presence in this country, the criminal may go free, but he should not go free within our borders.[131]

While courts today often read *Lopez-Mendoza*'s bar on suppression of identity evidence narrowly, consistent with its apparent limited application to jurisdiction over a defendant (Lopez-Mendoza, not Sandoval-Sanchez),[132] significant confusion lingers over whether identity evidence is categorically exempt from possible suppression.[133]

---

125. *Id.* at 1043.

126. *Id.* at 1044–45.

127. *Id.* at 1045.

128. *Id.* at 1046.

129. *Id.* at 1048–49.

130. *See id.* at 1046–47.

131. *Id.* at 1047.

132. *See, e.g.*, United States v. Olivares-Rangel, 458 F.3d 1104, 1111 (10th Cir. 2006) ("[T]he Supreme Court's statement [in *Lopez-Mendoza*] that the 'body' or identity of a defendant are 'never suppressible' applies only to cases in which the defendant challenges the jurisdiction of the court over him or her based upon the unconstitutional arrest, not to cases in which the defendant only challenges the admissibility of the identity-related evidence."); United States v. Guevara-Martinez, 262 F.3d 751, 753 (8th Cir. 2001) ("[T]he Court's reference to the suppression of identity [in *Lopez-Mendoza*] appears to be tied only to a jurisdictional issue, not to an evidentiary issue.").

133. *See* 6 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 11.4(g), at 449 (5th ed. 2012) ("[A]nother kind of 'fruit of the poisonous tree' question—one which has caused the courts particular difficulty—is whether identification evidence acquired following an illegal arrest is a tainted fruit of the arrest.").

While some courts allow exclusion under certain circumstances,[134] most categorically exempt identity evidence from exclusion.[135] The decision of the New York Court of Appeals in *People v. Tolentino*[136] is a prime example of the latter approach. In *Tolentino*, police unlawfully stopped a motorist, learned his name, conducted a search of Department of Motor Vehicles ("DMV") records, and learned that his license was suspended (and had been suspended in the past), resulting in his arrest for "aggravated unlicensed operation of a motor vehicle."[137]

The *Tolentino* court, citing *Lopez-Mendoza*, first proclaimed that identity evidence can never be subject to suppression,[138] and then the court addressed what it saw as the sole remaining issue: whether the defendant could successfully seek suppression of his DMV files, which were accessed as a result of the unlawful stop and demand of his identification.[139] The court refused to suppress the files because they "were obtained by the police from a source independent of the claimed illegal stop."[140]

The court then reiterated the various policy-based arguments against use of the exclusionary rule, and downplayed worry that police would be given an incentive to illegally seize individuals to secure identity evidence and access government database records.[141] According to the court, "[p]olice are already deterred from conducting illegal car stops because evidence recovered in the course of an illegal stop remains subject to the exclusionary rule."[142]

The court closed by distinguishing the Supreme Court's decisions in *Hayes v. Florida*[143] and *Davis v. Mississippi*,[144] noting that police in those cases illegally seized individuals to obtain fingerprints to link them to crimes actively being investigated, based on latent prints left at crime scenes.[145] In *Tolentino*, only a name was secured, and the exclusionary rule was inapplicable "when the only link between improper police activity and the disputed

134. *See, e.g.*, United States v. Oscar-Torres, 507 F.3d 224, 228–30 (4th Cir. 2007); *Olivares-Rangel*, 458 F.3d at 1111; United States v. Garcia-Beltran, 389 F.3d 864, 866 (9th Cir. 2004).

135. *See, e.g.*, United States v. Bowley, 435 F.3d 426, 430–31 (3d Cir. 2006) ("[W]e doubt that the Court lightly used such a sweeping word as 'never' in deciding when identity may be suppressed as the fruit of an illegal search of [sic] arrest.").

136. People v. Tolentino, 926 N.E.2d 1212 (N.Y. 2010), *cert. granted*, Tolentino v. New York, 562 U.S. 1043 (2010), *cert. dismissed*, 563 U.S. 123 (2011).

137. *Id.* at 1213.

138. *Id.* at 1214. The court emphasized that "[a] contrary holding would 'permit[] a defendant to hide who he is [and] would undermine the administration of the criminal justice system.'" *Id.* (second and third alterations in original) (quoting United States v. Farias-Gonzalez, 556 F.3d 1181, 1187 (11th Cir. 2009)).

139. *Id.*

140. *Id.* at 1216.

141. *Id.*

142. *Id.*

143. Hayes v. Florida, 470 U.S. 811, 815 (1985).

144. Davis v. Mississippi, 394 U.S. 721, 727 (1969).

145. *Tolentino*, 926 N.E.2d at 1216.

evidence is that the police learned the defendant's name."[146] Apparently oblivious to the important caveat in *Brown v. Texas* and *Hiibel* that police demand for identification is predicated on occurrence of a lawful seizure,[147] the majority opined that "[t]he Constitution does not prohibit the government from requiring a person to identify himself to a police officer."[148]

Ongoing uncertainty over *Lopez-Mendoza* promised to be rectified in November 2010 when the Supreme Court granted certiorari in *Tolentino*.[149] In a disjointed and meandering oral argument conducted the following spring, several Justices expressed obvious frustration over the government's refusal to recognize the constitutional importance of identity evidence. As Chief Justice Roberts said to government counsel, "you keep saying . . . you're just talking about the name[s], but names are meaningless in the abstract. It's not just that the officer wants to know what to call him. It's what he wants to find out from the name."[150] To Justice Alito, rather than addressing whether the government DMV records should be suppressed, "the simpler solution" was to suppress the officer's securing of identity information.[151] Ultimately, however, the Court dismissed the writ of certiorari as being improvidently granted,[152] leaving unresolved the question of whether the exclusionary rule applies when police unlawfully secure identity information and use the information to access a government database, resulting in the arrest of an individual.

C. *SUMMARY*

Attenuation doctrine (as applied in *Strieff*[153]) and the identity evidence exception serve as independent yet closely related bases allowing police to unlawfully secure identity information, access government databases, and search or seize individuals on the basis of information they discover. The doctrines have two foremost things in common. First, they overtly or tacitly import independent source doctrine, wrongly, to conclude that pre-existing government database information accessed by police cannot be causally connected to police wrongdoing. Second, they fail to apprehend the

146. *Id.*

147. *See* Hiibel v. Sixth Judicial Dist. Court, 542 U.S. 177, 184 (2004) (indicating "that the initial stop was based on reasonable suspicion, satisfying Fourth Amendment requirements"); *see also supra* notes 115–17 and accompanying text.

148. *Tolentino*, 926 N.E.2d at 1216.

149. Tolentino v. New York, 562 U.S. 1043 (2010).

150. Transcript of Oral Argument at 33, Tolentino v. New York, 562 U.S. 1043 (No. 09-11556) (statement of Roberts, C.J.); *see also id.* at 20 ("What should have been suppressed was the policeman's identification of the person who was driving the car." (statement of Scalia, J.)); *id.* at 34 ("[O]nce you get the guy's name you're interested in a lot of things." (statement of Roberts, C.J.)).

151. *Id.* at 21 (statement of Alito, J.) (stating rather than suppressing the government record, "suppress observations by the police on the scene that flow directly from the illegal stop").

152. Tolentino v. New York, 563 U.S. 123, 124 (2011).

153. *See supra* Section II.A.

constitutional importance of personal identifiers in modern-day policing. The next Part examines the practical significance of this failure.

III. THE CONSEQUENCES OF POLICE ACCESS

As noted earlier, police officers have long collected and relied upon information concerning individuals, especially those thought to pose criminal risk. This Part explores the broader implications of this reality, focusing first on arrest warrant databases like that accessed in *Strieff*, and thereafter examples of the myriad other kinds of databases now accessible to police.

A. ARREST WARRANTS

For the past several decades, state, local, and federal law enforcement agencies have contributed arrest warrant information to the National Criminal Information Center database.[154] An active arrest warrant entitles police to arrest an individual even when it is generated by another jurisdiction.[155] The vast majority of such warrants concern low-level offenses, such as neglecting to show up for a court date or pay a fee or fine (very often for a traffic offense),[156] or offenses of a quasi-criminal nature.[157]

Whatever the basis for an arrest warrant, an arrest is not only a traumatic experience in itself.[158] An arrest also allows police to search an arrestee's body,[159] which intrudes upon the personal privacy and "sanctity of the

---

154. *National Crime Information Center (NCIC)*, FBI, https://www.fbi.gov/services/cjis/ncic (last visited Oct. 23, 2018); *see also* David M. Bierie, *National Public Registry of Active-Warrants: A Policy Proposal*, 79 FED. PROB. 27, 28 (2015) ("The National Criminal Information Center (NCIC) is the central transactional data system that tracks the nation's warrants. All police agencies can enter their warrants in the system and check the system to identify whether a given individual has a warrant."). The NCIC also contains immigration-related information regarding individuals, which can result in civil and criminal violations. Laura Sullivan, Comment, *Enforcing Nonenforcement: Countering the Threat Posed to Sanctuary Laws by the Inclusion of Immigration Records in the National Crime Information Center Database*, 97 CALIF. L. REV. 567, 568 (2009). The records provide another basis for database "fishing expeditions."

155. Gabriel J. Chin & Marc L. Miller, *The Unconstitutionality of State Regulation of Immigration Through Criminal Law*, 61 Duke L.J. 251, 281–82 & n.136 (2011).

156. Research suggests that up to 75% of bench warrants for failure to appear concern traffic offenses. David M. Bierie, *Fugitives in the United States*, 42 J. CRIM. JUST. 327, 328 (2014).

157. *See* Wayne A. Logan, *After the Cheering Stopped: Decriminalization and Legalism's Limits*, 24 CORNELL J.L. & PUB. POL'Y 319, 341–43 (2014).

158. *See* United States v. Watson, 423 U.S. 411, 428 (1976) (Powell, J., concurring) (describing arrest as "a serious personal intrusion regardless of whether the person seized is guilty or innocent"); United States v. Marion, 404 U.S. 307, 320 (1971) (describing "[a]rrest [as] a public act that may seriously interfere with the defendant's liberty, . . . disrupt his employment, drain his financial resources, curtail his associations, subject him to public obloquy, and create anxiety in him, his family, and his friends").

159. *See* United States v. Robinson, 414 U.S. 218, 235 (1973). A lawful arrest also allows police to search the "area 'within [the arrestee's] immediate control.'" Chimel v. California, 395 U.S. 752, 763 (1969). If the arrestee is a recent occupant of a car, the car often can be searched. *See* Arizona v. Gant, 556 U.S. 332, 340–44 (2009).

person"[160] and has significant expressive harms.[161] When taken to a detention facility, which is often unsanitary and dangerous,[162] an arrestee can be subject to a strip search, even if no reason exists to suspect that they possess a weapon or contraband.[163] When being booked, arrestees can be forced to provide blood and DNA samples, containing highly personal information,[164] which the Supreme Court has acknowledged can foster "anxiety" among those targeted.[165] If an arrestee lacks money for bail—a very common occurrence even when it is set at a low amount[166]—detention can last several days or months.[167] One research study highlighted how prosecutors keep arrests open and require defendants to appear repeatedly in court,[168] allowing for "control" over them "without conviction."[169]

No less important, arrests have significant down-stream consequences. They negatively affect later criminal justice system outcomes,[170] impose a variety of immediate financial hardships,[171] and jeopardize current[172] and future employment.[173] It can also adversely affect housing, occupational licensure, and student loan opportunities,[174] impacting arrestees and their

160. Bond v. United States, 529 U.S. 334, 337 (2000) (quoting Terry v. Ohio, 392 U.S. 1, 17 (1968)).

161. Craig Konnoth, *An Expressive Theory of Privacy Intrusions*, 102 IOWA L. REV. 1533, 1535–36 (2017) (noting that searches by police "are harmful even if no damning information is found" because, inter alia, they "signal[] disrespect" and "that the state does not respect the boundaries that define her selfhood"); *id.* at 1536 ("[W]hen the state is the intruder, the intrusion can affect the way [the target] sees herself and her relationship with the state.").

162. *See, e.g.*, Matt Pearce, *Missouri Cities, Including Ferguson, Sued Over 'Grotesque' Jail Conditions*, L.A. TIMES (Feb. 9, 2015, 5:37 PM), http://www.latimes.com/nation/la-na-ferguson-lawsuit-20150209-story.html.

163. Florence v. Bd. of Chosen Freeholders, 566 U.S. 318, 324 (2012).

164. Birchfield v. North Dakota, 136 S. Ct. 2160, 2177–78 (2016).

165. *Id.* at 2178.

166. Nick Pinto, *The Bail Trap*, N.Y. TIMES MAG. (Aug. 13, 2015), https://www.nytimes.com/2015/08/16/magazine/the-bail-trap.html.

167. *See id.*

168. Issa Kohler-Hausmann, *Misdemeanor Justice: Control Without Conviction*, 119 AM. J. SOC. 351, 374, 378–81 (2013).

169. *Id.* at 351.

170. *See* Besiki Luka Kutateladze & Victoria Z. Lawson, *How Bad Arrests Lead to Bad Prosecution: Exploring the Impact of Prior Arrests on Plea Bargaining*, 37 CARDOZO L. REV. 973, 976 (2016) (explaining that arrest records are often considered in pretrial detention decisions, charge offers, and sentencing).

171. Wayne A. Logan & Ronald F. Wright, *Mercenary Criminal Justice*, 2014 U. ILL. L. REV. 1175, 1186–94.

172. Rachel A. Harmon, *Why Arrest?*, 115 MICH. L. REV. 307, 313–14 (2016); Eisha Jain, *Arrests as Regulation*, 67 STAN. L. REV. 809, 821–22 (2015).

173. *See, e.g.*, Benjamin D. Geffen, *The Collateral Consequences of Acquittal: Employment Discrimination on the Basis of Arrests Without Convictions*, 20 U. PA. J.L. & SOC. CHANGE 81, 85–86 (2017).

174. Wayne A. Logan, *Informal Collateral Consequences*, 88 WASH. L. REV. 1103, 1107–09 (2013).

dependents alike.[175] Finally, an arrest can result in physical harm[176] and even death,[177] and public shaming by having one's "mugshot" posted on a website.[178]

One might argue in response that wrongdoing is wrongdoing and that any violation of law should preclude grousing about negative consequences. As Rachel Harmon has observed, however, "[t]he consequences of arrests simply cannot be waved away on the ground that they are deserved."[179] Research has shown that court hearings for low-level offenses in particular are especially subject to repeated rescheduling, increasing the incidence of automatically issued "bench" arrest warrants for non-appearance.[180] Moreover, failure to appear is often the result of innocent mistake, such as being unaware of or forgetting the date for a court appearance, or is excusable, due to illness, inability to leave work, child care responsibilities, or unforeseen personal emergencies.[181] Also, significant court costs, system fees, and fines, can deter individuals from appearing.[182]

Deservedness becomes further strained when one considers the demographic skewing of arrest warrants issued for minor offenses. As Justice Kagan noted in *Utah v. Strieff*, such

> warrants are not distributed evenly across the population. To the contrary, they are concentrated in cities, towns, and neighborhoods where stops are most likely to occur—and so the odds of any given stop revealing a warrant are even higher than [the millions of

175. Harmon, *supra* note 172, at 316–17. Expunging or sealing an arrest record, when an opportunity is made available, can carry expense beyond the financial wherewithal of individuals, and the onus is upon them to initiate the process, which can be complicated and take considerable time and effort. Eisha Jain, *Proportionality and Other Misdemeanor Myths*, 98 B.U. L. REV. 953, 971–72 (2018).

176. *See, e.g.*, Roland G. Fryer, Jr., *An Empirical Analysis of Racial Differences in Police Use of Force* 3 (Nat'l Bureau of Econ. Research, Working Paper No. 22399, 2018) (noting resort by police to slapping, grabbing, and "pushing individuals into [the] wall or onto the ground"). Indeed, as the Supreme Court has noted, "an arrest or investigatory stop necessarily carries with it the right to use some degree of physical coercion or threat thereof to effect it." Graham v. Connor, 490 U.S. 386, 396 (1989).

177. *See* Devon W. Carbado & Patrick Rock, *What Exposes African Americans to Police Violence?*, 51 HARV. C.R.-C.L. L. REV. 159, 160–62 (2016) (citing recent instances of deadly force by police).

178. *See* Tim Stelloh, *Mugged!*, MARSHALL PROJECT (June 3, 2017, 2:30 PM), https://www.themarshallproject.org/2017/06/03/mugged (discussing mugshot websites operated by newspapers, police departments, and commercial entities).

179. Harmon, *supra* note 172, at 317.

180. *See* Issa Kohler-Hausmann, *Managerial Justice and Mass Misdemeanors*, 66 STAN. L. REV. 611, 658–59 (2014) (discussing results of a New York City study). According to counsel, in *Strieff* the arrest warrant for the traffic violation was "automatically" issued by the court. Transcript of Oral Argument of Joan C. Watt on Behalf of the Respondent at 52–53, Utah v. Strieff, 136 S. Ct. 2056 (2016) (No. 14-1373), 2016 WL 1028387, at *52–53.

181. Harmon, *supra* note 172, at 338.

182. *See* Meagan Cahill, *Focusing on the Individual in Warrant-Clearing Efforts*, 11 CRIMINOLOGY & PUB. POL'Y 473, 476 (2012) ("Court fees and other fines required to clear a warrant can also represent a financial hardship on some individuals and families, and it could be the root cause of leaving a warrant outstanding.").

> warrants in databases]. One study found, for example, that Cincinnati, Ohio had over 100,000 outstanding warrants with only 300,000 residents. And as Justice S[otomayor] notes, 16,000 of the 21,000 people residing in the town of Ferguson, Missouri have outstanding warrants.[183]

Even more troubling, according to a recent U.S. Department of Justice study, the municipal court in Ferguson issued arrest warrants "as a routine response to missed court appearances" in part because missed appearances generated more fines and fees.[184]

Arrest warrant databases, moreover, are known to contain erroneous information.[185] As Justice Ginsburg noted in *Herring v. United States*, a case involving an arrest (and incidental search) based on an invalid arrest warrant, "[t]he risk of error stemming from [warrant] databases is not slim,"[186] a point underscored by the fact that two recent U.S. Supreme Court decisions involved individuals wrongly arrested because of invalid warrants.[187]

Strieff, of course, involved a valid arrest warrant. When police act on an invalid warrant, and a wrongly arrested individual is not only subject to a bodily search—but is also strip-searched—intuition might dictate that a reviewing court would be outraged. However, the Court's decision in *Florence v. Board of Chosen Freeholders*[188] suggests otherwise. In a 5-4 decision, the Court condoned the strip searching of Albert Florence, who was a passenger in a car that was stopped for a minor traffic violation, and was arrested after the state trooper learned his identity and discovered an arrest warrant after running a warrants check.[189] The warrant, however, which was based on his alleged

183. Utah v. Strieff, 136 S. Ct. 2056, 2073 n.1 (2016) (Kagan, J., dissenting) (citations omitted).

184. CIVIL RIGHTS DIV., U.S. DEP'T OF JUSTICE, INVESTIGATION OF THE FERGUSON POLICE DEPARTMENT 3 (2015), https://www.justice.gov/sites/default/files/opa/press-releases/attachments/2015/03/04/ferguson_police_department_report.pdf [hereinafter DOJ, FERGUSON REPORT]. For further discussion of the tendency of governments to utilize the criminal justice system to generate revenue, see Logan & Wright, *supra* note 171, at 1176–77; *see also* Wayne A. Logan, *What the Feds Can Do to Rein in Local Mercenary Criminal Justice*, 2019 ILL. L. REV. (forthcoming 2019) (noting the particularly intractable challenges presented by revenue-generation among local criminal justice systems).

185. *See* Wayne A. Logan & Andrew Guthrie Ferguson, *Policing Criminal Justice Data*, 101 MINN. L. REV. 541, 559–60 (2016); Brandon V. Stracener, Note, *It Wasn't Me—Unintended Targets of Arrest Warrants*, 105 CALIF. L. REV. 229, 232–33 (2017).

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

187. *See* Florence v. Bd. of Chosen Freeholders, 566 U.S. 318, 323 (2012); Arizona v. Evans, 514 U.S. 1, 3–4 (1995). In *Evans*, the record indicated that on the day of defendant's unlawful arrest (based on a previously withdrawn warrant), three other similar arrests occurred in the same locality. *See Evans*, 514 U.S. at 28 (Ginsburg, J., dissenting).

188. *Florence*, 566 U.S. at 339–40.

189. *Id.* at 323.

failure to pay a fine, a form of contempt under New Jersey law, a non-criminal offense,[190] turned out to be invalid.

Florence informed the trooper that he had paid the fine two years before and presented a document stating proof of payment.[191] Without attempting to verify Florence's assertion, the trooper handcuffed Florence and transported him to jail,[192] where he was required to remove his clothes and ordered to open his mouth, lift his tongue and arms, and elevate his genitals for visual inspection.[193] Although no weapon or contraband was discovered, Florence remained in jail for six days.[194] He eventually was transferred to another county jail, where he again was strip searched,[195] told to open his mouth, lift his genitals, and turn around, squat and cough.[196]

The plurality opinion authored by Justice Kennedy,[197] and the concurrences of Chief Justice Roberts[198] and Justice Alito,[199] seemed unperturbed by the fact that Florence was wrongly arrested, leading to the major privacy and dignitary intrusions he suffered.[200] To Albert Florence, the experience "was humiliating. . . . [making him] feel less than a man. . . . not better than an animal."[201] The Justices, however, deemed the searches constitutionally reasonable based on the need of jail officials to search for weapons and contraband,[202] despite the menial basis for arrest and the absence of any individual suspicion of wrongdoing.[203]

---

190. *See* Petition for Writ of Certiorari at 4, Florence v. Bd. of Chosen Freeholders, 566 U.S. 318 (2012) (No. 10-945), 2011 WL 220710, at *4 [hereinafter Petition for Writ, Florence].

191. *Florence*, 566 U.S. at 323; Petition for Writ, Florence, *supra* note 190, at 3.

192. Petition for Writ, Florence, *supra* note 190, at 3–4 (noting that no ticket for the alleged traffic violation was issued and the basis for the initial stop was never specified).

193. *Florence*, 566 U.S. at 323.

194. *See id.*

195. *Id.* at 323–24.

196. *Id.* at 324.

197. *Id.* at 320.

198. *Id.* at 340 (Roberts, C.J., concurring).

199. *Id.* (Alito, J., concurring).

200. The procedure, as described by Justice Breyer in dissent, entailed "spreading and/or lifting [the subject's] testicles to expose the area behind them and bending over and/or spreading the cheeks of his buttocks to expose his anus. For females, the procedures are similar except females must in addition, squat to expose the vagina." *Id.* at 343 (Breyer, J., dissenting) (quoting Dodge v. County of Orange, 282 F. Supp. 2d 41, 46 (S.D.N.Y. 2003)).

201. Adam Liptak, *No Crime, but an Arrest and Two Strip-Searches*, N.Y. TIMES (Mar. 7, 2011), https://www.nytimes.com/2011/03/08/us/08bar.html.

202. *See Florence*, 566 U.S. at 337–39.

203. For a similarly disturbing instance of an arrest based on a "hit" to an arrest warrant database, involving an invalid warrant, see, for example, Bechman v. Magill, 745 F.3d 331, 332–33 (8th Cir. 2014). The facts, as recounted by the Eighth Circuit, were as follows:

> While the officers were in Bechman's home, Bechman told the officers she was breast feeding her infant daughter and she needed to use the bathroom because she was menstruating. The officers refused to allow Bechman to use the bathroom without the door open and one of the two male officers watching. . . . In addition,

In short, empowering police to unlawfully demand personal identifiers and access arrest warrants has major adverse consequences for individuals targeted. And worse yet, as *Florence* and the Court's prior decision in *Herring v. United States*[204] make clear, the accessed warrant—which often is for a very minor criminal or quasi-criminal offense—need not even be legally valid.

B. OTHER DATABASES

1. Stop, Arrest, and Conviction Records

Arrest warrants are not the only focus of databases. Another major component concerns information regarding the many millions of investigative stops[205] and arrests[206] conducted annually by police. Unlike in the past, when police-civilian contacts that did not result in conviction were destroyed,[207] today they are mainstays of government databases.

Stop and arrest records, and of course convictions, reflected in "rap sheets,"[208] have a self-replicating effect on the streets. Records accessed by police serve as new bases to stop, question, search and even arrest

---

> these male officers would not allow Bechman to exchange her breast milk soaked shirt for a dry one, or to put on a bra, unless one of them watched her change her clothes. She declined to do so.
>
> Leaving the baby with Bechman's husband, Officer Magill handcuffed Bechman, led her to his squad car, and drove her to the jail. At the jail, Bechman was strip searched and given a body cavity search. Bechman was detained at the jail overnight—the first time she had been separated from her nursing infant. The jailers released Bechman the next morning.

Id. at 333.

204. Herring v. United States, 555 U.S. 135, 147–48 (2009). In *Herring*, the Court allowed admission of evidence secured as the result of a search incident to arrest based on an invalid arrest warrant discovered in a government database. *Id.* at 137, 144. The majority held that the "good faith" exception to the exclusionary rule applies unless evidence exists that the error resulted from the department engaged in "deliberate, reckless, or grossly negligent conduct, or . . . recurring or systemic negligence" in maintaining the database. *Id.* at 142–44.

205. In New York City alone, police conducted "4.4 million stops between January 2004 and June 2012." Floyd v. City of New York, 959 F. Supp. 2d 540, 556 (S.D.N.Y. 2013).

206. It is estimated that over 13 million misdemeanor cases are filed annually in the United States. Megan Stevenson & Sandra Mayson, *The Scale of Misdemeanor Justice*, 98 B.U. L. REV. 731, 764 (2018).

207. *See supra* notes 43–51 and accompanying text.

208. JACOBS, *supra* note 10, at 9–10.

individuals,[209] fueling continued criminal justice system contacts.[210] According to one scholar, the records perform a marking function for police on street patrol, allowing those targeted to be sorted for future criminal justice system encounters.[211]

The records, however, have a contingent quality that must always be kept in mind. Stops, which overwhelmingly concern minor offenses,[212] are legally justified by "reasonable suspicion" of criminal activity,[213] a low proof quantum that is both readily manipulable and easy for police to satisfy.[214] It is also an unreliable indicator of actual criminal wrongdoing. Data concerning the long-running "stop and frisk" strategy of New York City police (January 2004–June 2012) are a case in point: police had a "hit rate" of 1.5% for discovery of weapons and only 6% resulted in arrests,[215] and nearly half of those arrests

209. *See, e.g.*, United States v. Wagers, 452 F.3d 534, 541 (6th Cir. 2006) (holding that knowledge of criminal history can help give rise to probable cause of current criminal activity); United States v. Sandoval, 29 F.3d 537, 542 (10th Cir. 1994) (holding that knowledge of prior criminal record can help create reasonable suspicion of current safety risk justifying a frisk); Roe v. Attorney Gen., 750 N.E.2d 897, 914 (Mass. 2001) ("A person's prior criminal record is a legitimate factor to consider in determining whether there is reasonable suspicion for a stop or probable cause for a search or an arrest.").

210. In some jurisdictions, police contacts are recorded to generate threat scores of individuals who come under the suspicion of police. *See* Justin Jouvenal, *The New Way Police Are Surveilling You: Calculating Your Threat 'Score,'* WASH. POST (Jan. 10, 2016), https://www.washingtonpost.com/local/public-safety/the-new-way-police-are-surveilling-you-calculating-your-threat-score/2016/01/10/e42bccac-8e15-11e5-baf4-bdf37355daoc_story.html. The more stops, the greater the likelihood of future stops. *See id.*; *see also, e.g.*, Jenn Rolnick Borchetta, *Curbing Collateral Punishment in the Big Data Age: How Lawyers and Advocates Can Use Criminal Record Sealing Statutes to Protect Privacy and the Presumption of Innocence*, 98 B.U. L. REV. 915, 926 (2018) ("The [New York City Police Department] has taken the position that it is permitted to use dismissed arrest information, and it has suggested it uses that information for a variety of law enforcement purposes." (footnote omitted)); Sarah Brayne, *Big Data Surveillance: The Case of Policing*, 82 AM. SOC. REV. 977, 989 (2017) (noting use of police-citizen contact data by Los Angeles police).

211. Kohler-Hausmann, *supra* note 180, at 614. *See generally* Jain, *supra* note 172 (noting variety of noncriminal justice actors who rely on arrests, including immigration enforcement officials, public housing authorities, employers, licensing authorities, and child protective service providers).

212. Bernard E. Harcourt & Tracey L. Meares, *Randomization and the Fourth Amendment*, 78 U. CHI. L. REV. 809, 820–21 (2011).

213. Terry v. Ohio, 392 U.S. 1, 30–31 (1968).

214. *See* Jeffrey Fagan & Amanda Geller, *Following the Script: Narratives of Suspicion in* Terry *Stops in Street Policing*, 82 U. CHI. L. REV. 51, 62, 86–87 (2015) (describing frequent resort by police to scripted "narratives" in justifying street stops); Eli B. Silverman, *With a Hunch and a Punch*, 4 J.L. ECON. & POL'Y 133, 134 (2007) (noting that even though they cannot serve as valid bases for stopping an individual, "police hunches" are "integral ingredients of police discretion, [and] are historically ingrained in the very nature of police work").

215. Floyd v. City of New York, 959 F. Supp. 2d 540, 558–59 (S.D.N.Y. 2013); Jeffrey Bellin, *The Inverse Relationship Between the Constitutionality and Effectiveness of New York City "Stop and Frisk,"* 94 B.U. L. Rev. 1495, 1511 (2014); Sharad Goel et al., *Combatting Police Discrimination in the Age of Big Data*, 20 NEW CRIM. L. REV. 181, 201 (2017).

did not result in conviction.[216] Similarly, a study of investigative detentions conducted by Newark, New Jersey police concluded that 93% lacked the requisite reasonable suspicion.[217]

In keeping with police deployment and street patrol strategies more generally,[218] data can also have a racial cast. In New York, stop-and-frisk data evidenced significant racial disparities,[219] a finding reflected in studies conducted elsewhere.[220] In an era of "predictive policing"—driven by algorithms based on aggregated past stops in particular areas driven by discretionary decisions of police[221]—race-based stops can have a self-replicating effect in communities.[222]

Arrest records are problematic for another reason. Given the undemanding requirement of probable cause,[223] and that police can arrest

---

216. ERIC T. SCHNEIDERMAN, N.Y. STATE OFFICE OF THE ATTORNEY GEN., A REPORT ON ARRESTS ARISING FROM THE NEW YORK CITY POLICE DEPARTMENT'S STOP-AND-FRISK PRACTICES 3, 10 fig.7 (2013), https://www.ag.ny.gov/pdfs/OAG_REPORT_ON_SQF_PRACTICES_NOV_2013.pdf.

217. CIVIL RIGHTS DIV., U.S. DEP'T OF JUSTICE, INVESTIGATION OF THE NEWARK POLICE DEPARTMENT 9 n.7 (2014), https://www.justice.gov/sites/default/files/crt/legacy/2014/07/22/newark_findings_7-22-14.pdf; *see also* David Rudovsky & David A. Harris, Terry *Stops-and-Frisks: The Troubling Use of Common Sense in a World of Empirical Data*, 79 OHIO ST. L.J. 501, 537 n. 231 (2018) (discussing results of Philadelphia study).

218. *See, e.g.*, Katherine Beckett et al., *Race, Drugs, and Policing: Understanding Disparities in Drug Delivery Arrests*, 44 CRIMINOLOGY 105, 129 (2006) (noting that "[p]redominantly white outdoor drug markets receive[d] far less attention" from police and "that the geographic concentration of law enforcement resources [was] a significant cause of racial disparity"); Nirej S. Sekhon, *Redistributive Policing*, 101 J. CRIM. L. & CRIMINOLOGY 1171, 1186–87 (2011) (discussing department policies regarding geographic deployment of officers, enforcement priorities, and tactics in proactive policing, resulting in disparate race and class-based impacts).

219. *See Floyd*, 959 F. Supp. 2d at 556 (noting that over 80% of the 4.4 million stops in the NYPD stop and frisk program were African-American or Latino). Despite being stopped more often, African-Americans and Latinos were less likely than whites to be in possession of contraband. *Id.* at 559. *See generally* AM. CIVIL LIBERTIES UNION, THE WAR ON MARIJUANA IN BLACK AND WHITE: BILLIONS OF DOLLARS WASTED ON RACIALLY BIASED ARRESTS (2013), https://www.aclu.org/report/report-war-marijuana-black-and-white (finding racial disparities in the marijuana arrest rates in all fifty states and the District of Columbia).

220. *See* I. Bennett Capers, *Race, Policing, and Technology*, 95 N.C. L. REV. 1241, 1255–57, 1269–70 (2017) (discussing studies conducted in inter alia Maryland, Minnesota, New Jersey and Pennsylvania).

221. *See* Josh Bowers, *Legal Guilt, Normative Innocence, and the Equitable Decision Not to Prosecute*, 110 COLUM. L. REV. 1655, 1699 (2010); Andrew Guthrie Ferguson, *Predictive Policing and Reasonable Suspicion*, 62 EMORY L.J. 259, 261 (2012).

222. *See* Elizabeth E. Joh, *Feeding the Machine: Policing, Crime Data, & Algorithms*, 26 WM. & MARY BILL RTS. J. 287, 300–01 (2017) ("By design . . . algorithms learn and reproduce the data they are given. If the data police provide to these systems already reflects a variety of priorities, filters, and decisions, then the results will too repeat those choices. And as police rely upon these predictive policing results to deploy their resources, they produce even more data that appear to confirm what the algorithm has predicted. That feedback loop reproduces a pattern of future policing, not future crime." (footnote omitted)).

223. *See* Illinois v. Gates, 462 U.S. 213, 246 (1983) (describing probable cause as "a fair probability" of wrongdoing).

for "a very minor criminal offense,"[224] and even quasi-civil offenses,[225] it should come as no surprise that one of every three adults can expect to be arrested by the age of 23.[226] It is clear, however, that high percentages of the many millions of arrests occurring annually do not result in prosecution much less conviction,[227] a critical detail that often goes unrecorded in criminal history databases.[228] Finally, even convictions, especially for misdemeanors and less serious offenses more generally, are very often less than they seem. This is because they frequently result from a haphazard system marked by innocents pleading guilty regardless of actual culpability.[229]

Police also use identity to access databases containing information on suspected gang members, also resulting in detention (or harassment).[230] At least 11 states and several large urban police departments, including New York City, have databases regarding suspected gang members,[231] which the FBI has collected and made available via the National Gang Intelligence

224. Atwater v. City of Lago Vista, 532 U.S. 318, 354 (2001).

225. *See* Logan, *supra* note 157, at 335–39.

226. Robert Brame et al., *Cumulative Prevalence of Arrest from Ages 8 to 23 in a National Sample*, 129 PEDIATRICS 21, 25 (2012). Rates are even higher among Hispanic (44%) and African-American (49%) males. Robert Brame et al., *Demographic Patterns of Cumulative Arrest Prevalence by Ages 18 and 23*, 60 CRIME & DELINQ. 471, 478 (2014). According to one recent study, more than 70 million individuals have criminal records of some kind. Matthew Friedman, *Just Facts: As Many Americans Have Criminal Records as College Diplomas*, BRENNAN CTR. FOR JUST. (Nov. 17, 2015), https://www.brennancenter.org/blog/just-facts-many-americans-have-criminal-records-college-diplomas.

227. *See, e.g.*, Andrew Golub et al., *The Race/Ethnicity Disparity in Misdemeanor Marijuana Arrests in New York City*, 6 CRIMINOLOGY & PUB. POL'Y 131, 147 (2007) (reporting a non-conviction rate of 80% for marijuana in public view ("MPV") arrests in New York City from 1992–2003); Kohler-Hausmann, *supra* note 180, at 641–43 (noting that in New York City, less than half of misdemeanor arrests in 2012 resulted in a conviction). From 2009 to 2016, nearly one fifth of felony arrests in California did not result in prosecution and almost one third did not result in a conviction. People v. Buza, 413 P.3d 1132, 1156 (Cal. 2018) (Liu, J., dissenting).

228. *See* Logan & Ferguson, *supra* note 185, at 566–67 ("In 2012, [for instance,] roughly seventeen million FBI background checks were conducted for employment and licensing purposes, yet, an estimated fifty percent of the FBI's records (provided by states) failed to include final disposition of arrest data, creating what are known as 'hanging arrests.'").

229. *See* Jain, *supra* note 172, at 822 (citing research showing routine entry of guilty pleas among persons facing misdemeanor charges "because it is too costly to contest charges at trial"); Jenny Roberts, *Why Misdemeanors Matter: Defining Effective Advocacy in the Lower Criminal Courts*, 45 U.C. DAVIS L. REV. 277, 308 (2011) (noting common tendency of individuals to plead guilty simply to secure release from jail, for instance to allow a return to work or to satisfy family demands). Recent data on misdemeanor exonerations show that a very high percentage of cases involved no criminal wrongdoing whatsoever, with data likely significantly under-counting actual occurrence because misdemeanor convictions seldom are subject to post-conviction review. Jenny Roberts, *The Innocence Movement and Misdemeanors*, 98 B.U. L. REV. 779, 810–11, 819 (2018).

230. Rebecca Rader Brown, Note, *The Gang's All Here: Evaluating the Need for a National Gang Database*, 42 COLUM. J.L. & SOC. PROBS. 293, 321 (2009).

231. Howell, *supra* note 4, at 15–16; Rebecca A. Hufstader, Note, *Immigration Reliance on Gang Databases: Unchecked Discretion and Undesirable Consequences*, 90 N.Y.U. L. REV. 671, 676–78 (2015).

Center since 2005.[232] The databases themselves have been the subject of widespread criticism because police independently designate individuals for inclusion, on the basis of often vague criteria that they are reluctant to disclose.[233] Usually, moreover, individuals are not even aware that they are in a database[234] and lack the ability to contest inclusion or seek confirmation that they have been purged.[235] This is so despite the recognized reality that the databases commonly contain errors.[236]

2. Biometric Data

Biometric data—including fingerprints, DNA and of late iris and facial images—are also collected, stored, analyzed, and accessed by police. Fingerprints are secured by police upon arrest, or provided voluntarily or inadvertently by individuals, and are readily available to police. The federally operated Automated Fingerprint Identification System ("AFIS") contains multiple million prints of criminal suspects and the "civil prints" of others, affording police quick and ready access to prints for use in identification.[237]

Databases also contain DNA profiles. The profiles are based on samples secured by police by any number of methods, including those voluntarily or inadvertently provided by individuals,[238] or based an arrest (for serious[239] and non-serious offenses alike[240]), often retained regardless of whether the

232. *See National Gang Intelligence Center*, FBI, https://www.fbi.gov/investigate/violent-crime/gangs/ngic (last visited Oct. 24, 2018).

233. *See* Kevin Lapp, *Databasing Delinquency*, 67 Hastings L.J. 195, 209–10 (2015).

234. Hufstader, *supra* note 231, at 680.

235. Lapp, *supra* note 233, at 211–12.

236. *See* Eric. J. Mitnick, *Procedural Due Process and Reputational Harm: Liberty as Self-Invention*, 43 U.C. DAVIS L. REV. 79, 126 (2009); Joshua D. Wright, *The Constitutional Failure of Gang Databases*, 2 STAN. J. C.R. & C.L. 115, 119–29 (2005). The Department of Homeland Security also uses gang databases to apprehend and remove noncitizen "known gang members," despite the known unreliability of the information. *See* Katherine Conway, Note, *Fundamentally Unfair: Databases, Deportation, and the Crimmigrant Gang Member*, 67 AM. U. L. REV. 269, 273–74 (2017). With a personal identifier, police can also access sex offender registries, similarly known to contain errors, that can result in arrest. *See* WAYNE A. LOGAN, KNOWLEDGE AS POWER: CRIMINAL REGISTRATION AND COMMUNITY NOTIFICATION LAWS IN AMERICA 110–14 (Stanford Univ. Press 2009); *see also, e.g.*, Sarsfield v. City of Marlborough, No. 03-10319-RWZ, 2006 WL 2850359, at *1 (D. Mass. Oct. 4, 2006) (concerning an individual who was exonerated but his name was not removed from the registry and who was threatened by police with arrest for not complying with registration requirement).

237. *Privacy Impact Assessment Integrated Automated Fingerprint Identification System National Security Enhancements*, FBI, https://www.fbi.gov/services/information-management/foipa/privacy-impact-assessments/iafis (last visited Sept. 18, 2018).

238. Elizabeth E. Joh, Maryland v. King: *Policing and Genetic Privacy*, 11 OHIO ST. J. CRIM. L. 281, 284 (2013).

239. Maryland v. King, 569 U.S. 435, 447–48 (2013) (allowing buccal extraction of DNA samples for "serious offense[s]").

240. *See* United States v. Buller, No. 4:17-CR-40105-KES, 2018 U.S. Dist. LEXIS 2202, at *14 (D.S.D. Jan. 5, 2018) (noting common interpretation of *King* to permit DNA samples from non-felony arrestees).

arrestee is charged or convicted.[241] DNA profiles are now being combined with other biometric identification data in the FBI's Next Generation Identification System,[242] the world's largest biometric database.[243] Police use such information in a manner not unlike the military, which seeks "identity dominance" on the battlefield.[244]

Biometric information, however, is also error-prone. Iris recognition is imperfect and risks false positives (i.e., misidentification of a party).[245] Facial recognition has similar reliability problems, especially with regard to women, people of color, and children,[246] with difficulties increasing when images are captured somewhere other than a controlled environment.[247] DNA, now the "gold standard" of biometric identification, can be undermined by a variety of factors, including its improper collection,[248] and even if not, can be subject to clerical or interpretive errors by technicians.[249]

DNA databases, moreover, are increasingly populated and operated by local governments with non-existent or modest quality controls,[250] fueled in part by profit-seeking commercial entities.[251] As noted earlier, jurisdictions also retain and use DNA information that should have been expunged or

241. *See* Kerry Abrams & Brandon L. Garrett, *DNA and Distrust*, 91 NOTRE DAME L. REV. 757, 778–79 (2015); Wayne A. Logan, *Government Retention and Use of Unlawfully Secured DNA Evidence*, 48 TEX. TECH L. REV. 269, 280 (2015).

242. *Next Generation Identification (NGI)*, FBI, https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ngi (last visited Oct. 24, 2018).

243. *See* Michael A. Cedrone, Note, *Technology's Effect on the Forty-Eight-Hour Rule and the Administrative Steps Incident to Arrest*, 69 RUTGERS U. L. REV. 289, 309 (2016).

244. Margaret Hu, *Biometric Cyberintelligence and the Posse Comitatus Act*, 66 EMORY L.J. 697, 744 (2017); *see also id.* at 724 (noting "the burgeoning of interoperable biometric databases and bureaucracies attempting to coordinate biometric cybersurveillance and biometric cyberintelligence strategies").

245. *See* Chantelle D. Ankerman, Note, *A Closer Look: Iris Recognition, Forensics, and the Future of Privacy*, 49 CONN. L. REV. 1357, 1365–66 (2017).

246. GEORGETOWN LAW CTR. ON PRIVACY & TECH., THE PERPETUAL LINE-UP: UNREGULATED POLICE FACE RECOGNITION IN AMERICA 53–54 (2016).

247. *See id.* at 29.

248. *See, e.g.*, Ken Strutin, *DNA Without Warrant: Decoding Privacy, Probable Cause and Personhood*, 18 RICH. J.L. & PUB. INT. 319, 347 (2015) ("Every stage in the collection, profiling, databanking and analysis of DNA evidence can be subject to human error, mechanical error, computer error, statistical error, false positives and cognitive biases."); Lauren Kirchner, *Traces of Crime: How New York's DNA Techniques Became Tainted*, N.Y. TIMES (Sept. 4, 2017), https://www.nytimes.com/2017/09/04/nyregion/dna-analysis-evidence-new-york-disputed-techniques.html.

249. ERIN E. MURPHY, INSIDE THE CELL: THE DARK SIDE OF FORENSIC DNA 140 (2015) (noting that audits of 22 of the roughly 190 laboratories nationwide revealed an error rate of six percent); Meghan J. Ryan & John Adams, *Cultivating Judgment on the Tools of Wrongful Conviction*, 68 SMU L. Rev. 1073, 1083 (2015) (discussing errors and reasons for their occurrence).

250. *See* Jason Kreag, *Going Local: The Fragmentation of Genetic Surveillance*, 95 B.U. L. REV. 1491, 1506–07, 1512–13 (2015); Stephen Mercer & Jessica Gabel, *Shadow Dwellers: The Underregulated World of State and Local DNA Databases*, 69 N.Y.U. ANN. SURV. AM. L. 639, 667–77 (2014).

251. Kreag, *supra* note 250, at 1506–19.

destroyed.[252] Finally, DNA databases, like stop, arrest and conviction databases, can reflect racially based policing practices,[253] which are likewise reproduced when police access and act upon database information.[254]

3. Unlawfully Secured Evidence

Databases can also contain information that was unlawfully secured by police. Despite the exhortation by the nation's leading Fourth Amendment scholar, Professor Wayne LaFave, that courts be "vigilant" in guarding against police efforts to populate their databases with information secured by illegal searches and seizures,[255] courts have backed their power to do so.

Perhaps the most influential decision on the question came in 1972 from the California Supreme Court in *People v. McInnis*.[256] In *McInnis*, Los Angeles police unlawfully arrested an individual for possessing a pistol and photographed him at booking.[257] One month later, police in nearby Pasadena showed the photo to a robbery victim who identified McInnis as the perpetrator.[258]

The *McInnis* court allowed use of the photo because "the illegal arrest was in no way related to the crime with which [the] defendant was ultimately charged"; it was "pure happenstance" that the photo secured by Los Angeles police was later used by Pasadena police to solve an unrelated crime.[259] Securing a photo during booking was "standard police procedure, bearing no relationship to the purpose or validity of the arrest or detention."[260] Furthermore, "[t]o hold that all such pictures resulting from illegal arrests are inadmissible forever . . . would allow the criminal immunity because another constable in another jurisdiction in another case had blundered. It

252. *See supra* note 241 and accompanying text.

253. Simon A. Cole, *Fingerprint Identification and the Criminal Justice System: Historical Lessons for the DNA Debate*, *in* DNA AND THE CRIMINAL JUSTICE SYSTEM: THE TECHNOLOGY OF JUSTICE 63, 82 (David Lazer ed., 2004).

254. As Kerry Abrams and Brandon Garrett observe more generally, government DNA collection efforts target "comparatively disadvantaged groups such as arrestees, convicts, juveniles, noncitizens, and welfare recipients," motivated by a desire to collect more genetic information. Abrams & Garrett, *supra* note 241, at 757–58. "In contrast, more privileged persons are not subjected to government DNA collection and may instead benefit from legislation protecting their genetic privacy." *Id.* at 759; *see also id.* at 804 ("[S]o long as minorities remain disproportionately subject to arrest as well as conviction, it is minorities that are most likely to be included in DNA databanks.").

255. 6 LAFAVE, *supra* note 133, § 11.4(g), at 463.

256. People v. McInnis, 494 P.2d 690 (Cal. 1972).

257. *Id.* at 691.

258. *Id.* at 690–91.

259. *Id.* at 692.

260. *Id.* (citation omitted).

would in effect be giving a crime insurance policy in perpetuity to all persons once illegally arrested . . . ."[261]

Justice Tobriner, echoing the concern voiced by the *Strieff* dissents decades later, warned in dissent:

> [L]aw enforcement officials stand to profit from illegal arrests. If these officials may use the direct fruits of illegal arrests in the prosecution of the individual for another offense, they will have a decided incentive to arrest anyone whom they "suspect" may be involved in illegal activity, regardless of whether that suspicion is legally sufficient for an arrest.[262]

As a consequence, he reasoned, "[m]ore innocent citizens will now face illegal arrest, and with it, the resulting disabilities of a [criminal] record."[263]

The *McInnis* scenario does not exhaust the avenues by which unlawfully secured evidence finds its way into government databases. Another involves when agents of one government secure evidence unlawfully, based on the sovereign's law, making it inadmissible in court, yet the evidence is given to agents of another sovereign where the police activity was proper, making the evidence admissible in the latter's courts.[264] For instance, state or local police might seize evidence in violation of a state constitutional requirement, affording federal agents the opportunity to use the same evidence against the individual in a federal criminal prosecution.[265]

Yet another scenario involves what has been referred to as "laundering" of unlawfully secured evidence.[266] Such a situation occurs when one officer unlawfully secures evidence and another officer (possibly from the same jurisdiction), with no or limited knowledge of the initial illegality, discovers or relies upon the tainted evidence. Courts, invoking *Herring v. United States*,[267] admit the evidence based on the "good faith" exception to the exclusionary

---

261. *Id.* at 693; *see also* United States v. Cella, 568 F.2d 1266, 1285–86 (9th Cir. 1978), *amended by* 568 F.2d 1266 (9th Cir. 1978) ("[T]o grant life-long immunity from investigation and prosecution simply because a violation of the Fourth Amendment first indicated to the police that a man was not the law-abiding citizen he purported to be would stretch the exclusionary rule beyond tolerable bounds." (quoting United States v. Friedland, 441 F.2d 855, 861 (2d Cir. 1971)).

262. *McInnis*, 494 P.2d at 695 (Tobriner, J., dissenting). For results of a field survey reflecting frank acknowledgment of this motivation among local law enforcement, with regard to the collection of DNA, see Kreag, *supra* note 250, at 1512–13.

263. *McInnis*, 494 P.2d at 695 (Tobriner, J., dissenting).

264. *See generally* Wayne A. Logan, *Dirty Silver Platters: The Enduring Challenge of Intergovernmental Investigative Illegality*, 99 IOWA L. REV. 293 (2013) (discussing ways in which state and federal agents can avoid otherwise applicable limits on their authority).

265. *See id.* at 309–16 (citing examples from the caselaw).

266. *See* Kay L. Levine et al., *Evidence Laundering in a Post-*Herring *World*, 106 J. CRIM. L. & CRIMINOLOGY 627, 642–58 (2016) (detailing ways in which unlawfully obtained evidence can be "laundered" and later used by police).

267. Herring v. United States, 555 U.S. 135 (2009).

rule.[268] In such a situation, evidence is allowed to be "magically resuscitate[d] . . . phoenix-like."[269] According to the authors of a recent study, the behavior is thought to be especially likely in the database context: "When the original error involves the faulty assembly or maintenance of an arrest warrant database, DNA database, vehicle registration database, or some comparable collection of information for law enforcement purposes, the good faith exception almost always carries the day . . . ."[270]

4. Sensitive Personal Information

Finally, personal identifiers afford police access to databases containing sensitive information regarding individuals. While arrest and conviction records, home addresses and the like certainly are not information that individuals typically are happy to have revealed, the information is "public" in the sense that it is publicly available.[271] Law enforcement databases, however, contain a wealth of information that is of a decidedly more personally sensitive nature.[272]

The National Crime Information Center, which as discussed earlier is accessed by state, local, and federal law enforcement nationwide,[273] affords an example. Although the NCIC originated over fifty years ago to centralize criminal justice records, it has long since expanded to include sensitive personal information. For instance, in addition to indicating whether an individual has a scar or tattoo, it can reflect whether they have extra body parts (e.g., "EXTR BRST," "EXTR NIP"), missing body parts (e.g., "MISS BRSTS," "MISS PENIS," "MISS UTRUS"), implants ("ART BRSTS," "IMPL PENIS"), eating disorders ("MC EATDIS"), substance abuse problems (e.g., "DA GLUE"), pregnancies ("MC PASTPRE"), pierced body parts ("PRCD GNTLS"), and whether they have used anti-depressants ("TD ADEPRES").[274]

---

268. As the authors point out, however, the scenario does not always involve more than one officer. *See* Levine et al., *supra* note 266, at 642 n.78 ("[F]inding a good faith mistake where an officer reasonably relied on his own erroneously obtained information." (citing United States v. Massi, 761 F.3d 512, 529–32 (5th Cir. 2014))).

269. *Id.* at 646 (alteration in original) (quoting People v. Ramirez, 668 P.2d 761, 764 (Cal. 1983)).

270. *Id.* at 656; *see also id.* at 659 ("Officers in one jurisdiction now have an incentive to pass along tainted evidence to officers in another jurisdiction, without revealing problems in the evidence collection process, because the good faith doctrine will insulate their handoff.").

271. Indeed, courts have often stated that the nominally public information aggregated on sex offender registries—e.g., names, vehicle descriptions, home and work addresses, and criminal history—is not deserving of privacy protection. *See* LOGAN, *supra* note 236, at 141–47.

272. On the more general definitional question of what does and should qualify as "sensitive" information, and the legal limits on its collection, access and use, see Paul Ohm, *Sensitive Information*, 88 S. CAL. L. REV. 1125, 1132–36 (2015).

273. *See supra* note 154 and accompanying text.

274. NAT'L CRIME INFO. CENT., NCIC CODE MANUAL AS OF SEPTEMBER 30, 2017, at 26–27, 29, 30–31, 37, 40–42 (2017), https://www.oregon.gov/osp/CJIS/docs/NCIC%20Manuals/2017/NCICCodeManual_FULL.pdf.

DNA databases also store personally sensitive information. DNA samples are processed to create a profile consisting of "junk DNA," which is generally thought to not include sensitive genetic information.[275] Not all researchers agree, however, that "junk DNA" is incapable of revealing health or personal matters.[276] Because governments often do not destroy DNA samples used to create profiles,[277] retention of samples raises the possibility[278] of sensitive genetic details (such as racial ancestry, predisposition to serious diseases) being discovered.[279] Very recently, the Supreme Court spoke to this concern, in the analogous context of government retention of blood samples:

> a blood test . . . places in the hands of law enforcement authorities a sample that can be preserved and from which it is possible to extract information beyond a simple BAC reading. Even if the law enforcement agency is precluded from testing the blood for any purpose other than to measure BAC, the potential remains and may result in anxiety for the person tested.[280]

Exacerbating matters, to the extent that government databases are susceptible to hacking or other wrongful access, question exists over whether civil redress is available to individuals suffering the negative consequences of a data breach.[281]

---

275. Simon A. Cole, *Is the "Junk" DNA Designation Bunk?*, 102 NW. U. L. REV. COLLOQUY 54, 56–57 (2007).

276. *See* Meghan J. Ryan, *The Privacy, Probability, and Political Pitfalls of Universal DNA Collection*, 20 SMU SCI. & TECH. L. REV. 3, 13–15 (2017). Several scholars, moreover, have raised concern over the eventual use of DNA to create profiles suggestive or criminal predisposition. *Id.* at 15 (providing examples of ways "junk DNA" could be misused).

277. *See supra* note 241 and accompanying text.

278. Jurisdictions might also be engaged in the creation of "rogue" databases, entailing "the collection and recording of samples of samples in local and unofficial databases that need not comply with formal statutory law." Erin Murphy, Comment, *License, Registration, Cheek Swab: DNA Testing and the Divided Court*, 127 HARV. L. REV. 161, 172 (2013). *See generally* Kreag, *supra* note 250 (discussing proliferation of local government DNA databases created and operated by private companies operating beyond the reach of federal requirements).

279. Indeed, caselaw concluding that government testing of samples in its possession does not qualify as a "search," precluding need for a warrant, would allow for this. *See generally* Tracey Maclin, *Government Analysis of Shed DNA Is a Search Under the Fourth Amendment*, 48 TEX. TECH. L. REV. 287 (2015).

280. Birchfield v. North Dakota, 136 S. Ct. 2160, 2178 (2016); *see also* People v. Buza, 413 P.3d 1132, 1174 (Cal. 2018) (Cuéllar, J., dissenting) ("The DNA profile maintained in state and federal databases thus has the potential to reveal vast amounts of personal information about . . . individuals, and to be used in ways starkly different relative to what justified the scheme."). Iris recognition technology raises similar concern. *See, e.g.*, Patrick J. Morrison, Jr., *The Iris—A Window into the Genetics of Common and Rare Eye Diseases*, 79 ULSTER MED. J. 3, 3–5 (2010) (noting that some chromosome disorders such as Down Syndrome can be detected by iris patterns).

281. *Cf.* Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737, 780–86 (2018) (discussing tendency of courts to deny standing to individuals suffering data breaches, creating risk of identity theft and the like, based on view that harm is uncertain and intangible).

Finally, in a time when it is difficult to determine the nature and extent of personal information stored in government databases, including from commercial businesses one has patronized and the "internet of things,"[282] liberating police to access such information should raise concern. Indeed, examples of problematic yet undetected police practices are not hard to find. For many years, for instance, state and federal law enforcement created and participated in a website "known as the Black Asphalt Electronic Networking & Notification System," which "received no oversight by government, even though its reports contained law enforcement sensitive information about traffic stops and seizures, along with hunches and personal data about drivers, including Social Security numbers and identifying tattoos."[283] In Rochester, Minnesota, police not only learn whether a person detained has a criminal record, but also whether they were ever associated with someone with a record (including a romantic partner).[284] Massachusetts state troopers, equipped with a name, access information ranging from unlisted phone numbers to roommates.[285] And it took a public records request to learn that one of the Fresno Police Department's predictive software algorithms used the social media hashtag #BlackLivesMatter as a risk factor for "police hate crimes."[286]

C. *IMPLICATIONS*

Police use of personal identity to access database information has significant consequences for individuals and the communities in which they live. Arrests, triggered by database access can have life-changing negative

282. *See* Andrew Guthrie Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 CALIF. L. REV. 805, 818–23 (2016); Scott J. Shackelford et al., *When Toasters Attack: A Polycentric Approach to Enhancing the "Security of Things,"* 2017 U. ILL. L. REV. 415, 429–36.

283. Robert O'Harrow Jr. et al., *Police Intelligence Targets Cash: Reports on Drivers, Training by Firm Fueled Law Enforcement Aggressiveness*, WASH. POST (Sept. 7, 2014), https://www.washingtonpost.com/sf/investigative/2014/09/07/police-intelligence-targets-cash.

284. Maya Rao, *Rochester Hopes Predictive Policing Can Steer Juveniles Away from Crime*, STAR TRIB. (Oct. 24, 2014, 11:18 PM), http://www.startribune.com/rochester-police-plan-to-target-at-risk-teens-raises-concerns/280385202.

285. Keith Reed, *Logan Troopers to Get Roving Database Access: Access Critics See Threat to Privacy Rights in Antiterrorism Move*, BOSTON GLOBE (June 22, 2004), http://archive.boston.com/business/technology/articles/2004/06/22/logan_troopers_to_get_roving_database_access. According to a corporate executive at the company that collected such information and provided it to police: "'[a] name, that's all [an officer] needs' . . . . '[to] find out who you lived with, where you lived, anything about you.'" *Id.*; *see also, e.g.*, Sadie Gurman, *Across US, Police Officers Abuse Confidential Databases*, WIS. ST. J. (Oct. 3, 2016), https://madison.com/wsj/news/local/crime-and-courts/across-us-police-officers-abuse-confidential-databases/article_9e73c669-b8f2-5701-9ee1-9b9572adb7e4.html (describing how law enforcement has misused confidential databases).

286. Andrea Castillo, *ACLU Slams Fresno Police for Testing Social Media Surveillance Software*, FRESNO BEE (Jan. 2, 2016, 4:38 PM), https://www.fresnobee.com/news/local/article52549320.html; *see also* Tim Sheehan, *Fresno Council Halts Purchase of Data Software Wanted by Police*, FRESNO BEE (Apr. 1, 2016, 1:45 PM), https://www.fresnobee.com/news/local/article69337677.html (explaining that software allows police to track threats based on specific hashtags used on social media).

consequences for those targeted.[287] So can investigative detentions, which the Supreme Court has described as "a serious intrusion upon the sanctity of the person, which may inflict great indignity and arouse strong resentment,"[288] a recognition backed by a substantial body of research highlighting the adverse physical and psychological consequences of stops.[289]

With police already motivated to stop and arrest by significant individual and institutional pressures in the name of "productivity,"[290] "'bigger' busts,"[291] and overtime pay,[292] enabling them to make more of them should prompt concern.[293] So too should the recognized tendency of governments to regard police street patrol as an opportunity for revenue-generation[294] and for arrest volumes themselves to serve as a funding metric.[295] Finally, as discussed

287. *See supra* Section III.A.

288. Terry v. Ohio, 392 U.S. 1, 17 (1968); *see also* Heien v. North Carolina, 135 S. Ct. 530, 544 (2014) (Sotomayor, J., dissenting) (referring to stops as "invasive, frightening, and humiliating" experiences).

289. Josephine Ross, *Warning: Stop-and-Frisk May Be Hazardous to Your Health*, 25 WM. & MARY BILL RTS. J., 689, 726–28 (2016) (discussing studies highlighting such effects). The negative consequences of which, research has shown, are exacerbated by the fact that they occur in public spaces. *See* Alexander A. Reinert, *Public Interest(s) and Fourth Amendment Enforcement*, 2010 U. ILL. L. REV. 1461, 1489 (citing a study of the New York City Police Department).

290. *See, e.g.*, Harmon, *supra* note 172, at 360 (noting that police departments "use arrest numbers as a measure of productivity"); Saki Knafo, *How Aggressive Policing Affects Police Officers Themselves*, ATLANTIC (July 13, 2015), https://www.theatlantic.com/business/archive/2015/07/aggressive-policing-quotas/398165 (discussing widespread use of arrest quotas and their use in officer evaluations); *see also* Elina Treyger, *Collateral Incentives to Arrest*, 63 U. KAN. L. REV. 557, 558, 564–67 (2015) (discussing broader non-criminal justice-related functions of arrest and noting that "[t]he rise of increasingly encompassing and interoperable databases presents a tantalizing opportunity to combine criminal law enforcement with other public policy goals," including securing biometric information, increasing productivity metrics of police, and facilitating immigration enforcement).

291. *See* Wayne A. Logan, *Cutting Cops Too Much Slack*, 104 GEO. L.J. ONLINE 87, 90–91 (2015); *see also* BERNARD E. HARCOURT, ILLUSION OF ORDER: THE FALSE PROMISE OF BROKEN WINDOWS POLICING 10 (2001) (quoting William Bratton, Commissioner of the NYPD: "Every [minor offense] arrest [is] like opening a box of Cracker Jack. What kind of toy am I going to get? Got a gun? Got a knife? Got a warrant? . . . It [is] exhilarating for the cops.").

292. *See* Cordero v. City of New York, 282 F. Supp. 3d 549, 555 n.2 (E.D.N.Y. 2017) (citing news reports describing police resorting to arrests to secure overtime pay for time associated with administrative processing of arrests).

293. *See* Rachel A. Harmon, *The Problem of Policing*, 110 MICH. L. REV. 761, 792 (2012) (advocating "harm-efficient policing": "policing that imposes harms only when, all things considered, the benefits for law, order, fear reduction, and officer safety outweigh the costs of those harms").

294. *See* Logan & Wright, *supra* note 171, at 1185.

295. *See, e.g.*, Karena Rahall, *The Green to Blue Pipeline: Defense Contractors and the Police Industrial Complex*, 36 CARDOZO L. REV. 1785, 1800 n.103 (2015) (noting that federal grant money has been tied "to departments based entirely on the number of drug arrests made by each department and drug arrests skyrocketed as a result").

earlier, database information accessed by police can be inaccurate[296] or of a personally sensitive or embarrassing nature.[297]

The broader societal implications of this authority are no less consequential. As others have noted, the Fourth Amendment's assurance of the right of "the people" to be "secure" guards against more than actual unreasonable searches and seizures—it guards the right to be free of apprehension that they will occur.[298] Justice Sotomayor, in her concurring opinion in *United States v. Jones*, expressed this concern when she warned that increasing governmental capacity to collect, store, and analyze data risks the chilling of "associational and expressive freedoms."[299]

Already, in many places, especially poor and minority communities subject to aggressive proactive policing strategies,[300] concern exists that anxieties about potential police encounters will discourage community members' willingness to venture outside and engage in civic life.[301] In a community such as Ferguson, Missouri, where an arrest warrant (most often for a failure to appear or pay the accumulating exorbitant fees racked up for municipal code violations) existed for 75% of the adult population,[302] such trepidation quite understandably existed.[303] DOJ investigators found that Ferguson police regularly detained individuals without legal justification to

296. *See, e.g.*, *supra* notes 185–87, 215–36, 248–49 and accompanying text.

297. *See supra* notes 271–86 and accompanying text.

298. *See, e.g.*, Luke M. Milligan, *The Forgotten Right to be Secure*, 65 HASTINGS L.J. 713, 746 (2014); Jed Rubenfeld, *The End of Privacy*, 61 STAN. L. REV. 101, 122 (2008); Richard H. McAdams, Note, *Tying Privacy in* Knotts*: Beeper Monitoring and Collective Fourth Amendment Rights*, 71 VA. L. REV. 297, 318–19 (1985).

299. United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring); *see also* Rubenfeld, *supra* note 298, at 127 (defining insecurity as "the stifling apprehension and oppression that people would justifiably experience if forced to live their personal lives in fear of appearing 'suspicious' in the eyes of the [governmental authorities]"). For social science research supporting this point, see Nicole B. Cásarez, *The Synergy of Privacy and Speech*, 18 U. PA. J. CONST. L. 813, 853–59 (2016).

300. *See* Aziz Z. Huq, *The Consequences of Disparate Policing: Evaluating Stop and Frisk as a Modality of Urban Policing*, 101 MINN. L. REV. 2397, 2411–12 (2017) (surveying data evidencing the most common focus of stop, question and frisk policing).

301. Amy E. Lerman & Vesla M. Weaver, *Staying Out of Sight? Concentrated Policing and Local Political Action*, 651 ANNALS AM. ACAD. POL. & SOC. SCI. 202, 205 (2014); Robert J. Sampson, *When Things Aren't What They Seem: Context and Cognition in Appearance-Based Regulation*, 125 HARV. L. REV. F. 97, 105 (2012); *see also* Reinert, *supra* note 289, at 1489 ("A public Fourth Amendment intrusion leaves an impression, especially one that is perceived as wrongful or unjustified. It reinforces the lack of control that an individual has over where and when he is going when he is in public." (footnotes omitted)).

302. *See* DOJ, FERGUSON REPORT, *supra* note 184, at 6, 55.

303. *See* Jelani Cobb, *What I Saw in Ferguson*, NEW YORKER (Aug. 14, 2014), https://www.newyorker.com/news/news-desk/saw-ferguson (recounting statement provided by Ferguson resident: "'We have people who have warrants because of traffic tickets and are effectively imprisoned in their homes . . . . They can't go outside because they'll be arrested. In some cases people actually have jobs but decide the threat of arrest makes it not worth trying to commute outside their neighborhood.'").

run names in their municipal arrest warrant database.[304] Police also accessed a separate "wanted" persons database based on belief that probable cause existed to arrest (without judicial review).[305] Wanted orders were also issued in the absence of probable cause and otherwise were imprecise or inaccurate.[306]

And, even if community members are confident that absolutely no basis for arrest exists in a database, they might be wary of the new authority of police (per *Strieff*[307]) to unlawfully seize individuals and demand identity information to see if an arrest basis might possibly be stored in a database.[308] They might also be aware of the ready way in which a stop, even if unlawful, can morph into a lawful basis for arrest, such as when an officer thinks they are being uncooperative (i.e., committing "contempt of cop")[309] or engaging in any of the multitude of other forms of minor and quasi-criminal misconduct,[310] which can serve as a basis to attenuate taint.[311] In short, *Strieff* significantly undercut what the Court itself has extolled as the constitutional "right to go

304. *See* DOJ, FERGUSON REPORT, *supra* note 184, at 49, 56–57. As the DOJ, Ferguson Report highlighted, most often the offense triggering an arrest warrant was based on the local municipal code, not the state code, "even when an analogous state offense exist[ed]." *Id.* at 7. Jurisdiction therefore existed in the Ferguson Municipal Court, which operated as part of the police department, the revenue-motivated procedures and processes of which prompted major concern for investigators. *Id.* at 8–15.

305. *Id.* at 22 ("[W]anteds . . . operate as an end-run around the judicial system. . . . [O]fficers make the probable cause determination themselves and circumvent the courts. Officers use wanteds for serious state-level crimes and minor code violations alike, including traffic offenses.").

306. *Id.* at 23 (according to the DOJ investigators, the "system creates the risk that wanteds could be used improperly to develop evidence necessary for arrest rather than to secure a person against whom probable cause already exists").

307. *See supra* notes 71–105 and accompanying text.

308. What Jane Bambauer recently called being subject to "hassle": "the chance that the police will stop or search an innocent person against his will." Jane Bambauer, *Hassle*, 113 MICH. L. REV. 461, 464 (2015).

309. *See* DOJ, FERGUSON REPORT, *supra* note 184, at 21–22, 25 (noting how Ferguson police commonly demanded identification from individuals, without legal justification, and that if individuals refused they would be arrested for "Failure to Comply," consistent with their training); Christy E. Lopez, *Disorderly (mis)Conduct: The Problem with "Contempt of Cop" Arrests*, 4 J. AM. CONST. SOC'Y FOR L. & POL. 71 (2010) (noting the prevalence of disorderly conduct arrests when an individual resisted perceived police misconduct); *see also, e.g.*, United States v. Shepherd, 160 F. App'x. 489, 491–92 (7th Cir. 2005) (noting that even if police lacked probable cause to undertake warrantless arrest, they had probable cause to believe that the defendant resisted law enforcement, justifying arrest and search incident to arrest).

310. *See* Logan, *supra* note 157, at 336–39 (surveying vast discretionary arrest authority afforded police by *Atwater v. City of Lago Vista*, 532 U.S. 318 (2001)).

311. 6 LAFAVE, *supra* note 133, § 11.4(j), at 483–91 (discussing the "new-crime" doctrine). And, because police can influence prosecutors' charging and plea bargaining, and in some instances even file charges and prosecute cases themselves, such arrests can readily translate into convictions. *See* Jonathan Abel, *Cops and Pleas: Police Officers' Influence on Plea Bargaining*, 126 YALE L.J. 1730, 1769–73 (2017); Nikolas Frye, Note, *Allowing New Hampshire Police Officers to Prosecute: Concerns with the Practice and a Solution*, 38 NEW ENG. J. ON CRIM. & CIV. CONFINEMENT 339, 340 (2012).

about one's business free from unwarranted government interference."[312] One best be a compliant "good citizen"[313] and submit to an officer's unlawful demand for identity, not a "rugged individual" who sticks up for his right to not acquiesce.[314]

Research shows that the disengagement fueled by such police behaviors can have toxic effect on communities, reducing neighborhood collective efficacy[315] and the willingness of individuals to assist police.[316] In such an environment, even the factually innocent—"the . . . group for whom the Fourth Amendment's protections ought to be most jealously guarded"[317] —can be deterred from going places, engaging in certain behaviors or assembling with fellow citizens.[318] Moreover, to the extent that government databases contain information on political affiliation or involvement,[319] one can expect lowered willingness to render oneself vulnerable to police targeting.[320] One might also be averse to having police access information of

312. Immigration & Naturalization Serv. v. Delgado, 466 U.S. 210, 226 (1984).

313. I. Bennett Capers, *Criminal Procedure and the Good Citizen*, 118 COLUM. L. REV. 653, 654 (2018).

314. Scott E. Sundby, *The Rugged Individual's Guide to the Fourth Amendment: How the Court's Idealized Citizen Shapes, Influences, and Excludes the Exercise of Constitutional Rights*, 65 UCLA L. REV. 690, 694 (2018).

315. Robert J. Sampson, *Neighborhood Effects, Causal Mechanisms and the Social Structure of the City*, *in* ANALYTICAL SOCIOLOGY AND SOCIAL MECHANISMS 227, 232 (Pierre Demeulenaere ed., 2011) (defining collective efficacy as "the linkage of mutual trust and the shared willingness to intervene" in criminal or anti-social activity); *see also* Jeffrey D. Morenoff et al., *Neighborhood Inequality, Collective Efficacy, and the Spatial Dynamics of Urban Violence*, 39 CRIMINOLOGY 517, 520 (2001) (defining "collective efficacy" as "linkage of trust and cohesion with shared expectations for control").

316. NANCY LA VIGNE ET AL., URBAN INST., HOW DO PEOPLE IN HIGH-CRIME, LOW-INCOME COMMUNITIES VIEW THE POLICE? 10–11 (2017), https://www.urban.org/sites/default/files/publication/88476/how_do_people_in_high-crime_view_the_police.pdf; Huq, *supra* note 300, at 2432–35; Tom R. Tyler, *From Harm Reduction to Community Engagement: Redefining the Goals of American Policing in the Twenty-First Century*, 111 NW. U. L. REV. 1537, 1549–54 (2017).

317. Maryland v. King, 569 U.S. 435, 482 (2013) (Scalia, J., dissenting).

318. *See* LU-IN WANG, DISCRIMINATION BY DEFAULT: HOW RACISM BECOMES ROUTINE 104 (Richard Delgado & Jean Stefancic eds., 2006) (noting that minorities in particular engage in aversive behaviors "to avoid . . . detain[ment] becom[ing] a part of their daily routines" (emphasis omitted)); L. Rush Atkinson, *The Bilateral Fourth Amendment and the Duties of Law-Abiding Persons*, 99 GEO. L.J. 1517, 1520 (2011) (noting how "[t]he limited nature of constitutional protections against government searches . . . [can] deter[] law-abiding persons from engaging in behavior that is not barred under the criminal code"); Christopher Slobogin, *The Poverty Exception to the Fourth Amendment*, 55 FLA. L. REV. 391, 405 (2003) (noting "that many poor people, especially African American ones in certain urban areas, do not want to deal with the police even when innocent of any crime").

319. *See, e.g.*, *supra* note 286 and accompanying text (describing database reference to individual's involvement in "Black Lives Matter").

320. The Supreme Court itself has long recognized the risks of harassment associated with knowledge of political affiliation. *See* Brown v. Socialist Workers '74 Campaign Comm., 459 U.S. 87, 101–02 (1982) ("The First Amendment prohibits a state from compelling disclosures by a minor party that will subject those persons identified to the reasonable probability of threats, harassment or reprisals. Such disclosures would infringe the First Amendment rights of the party and its members and supporters."); Bates v. City of Little Rock, 361 U.S. 516, 523 (1960) (denying

an embarrassing or personally sensitive nature,[321] even if the information does not result in an arrest or search.

In short, empowering and incentivizing police to unlawfully seize individuals not only undercuts basic rule of law values;[322] it also chills individuals' ability to engage in the self-planning necessary to act freely and autonomously in a democratic society.[323]

Finally, allowing for and encouraging unlawful stops can have negative structural effects on entire communities.[324] Research consistently shows a positive correlation between increased police contacts and reduced social and economic capital, which can promote socio-economic stratification and isolation[325] and have an overall destructive impact on neighborhoods.[326] As Richard Bierschbach and Stephanos Bibas recently noted, police officers and departments benefit strategically from aggressive proactive street patrol, but they often "do not suffer the costs they individually and collectively impose upon others."[327] Limiting police authority to unlawfully demand personal identifiers and access database information will mitigate these negative externalities.

---

required disclosure of NAACP membership lists because freedom of association and speech "are protected not only against heavy-handed frontal attack, but also from being stifled by more subtle governmental interference").

321. *See supra* notes 271–86 and accompanying text.

322. *See* Wayne A. Logan, *Police Mistakes of Law*, 61 EMORY L.J. 69, 90–93 (2011) (discussing the ways in which unlawful police seizures undercut individuals' freedom of movement and autonomy).

323. *See* H.L.A. HART, PUNISHMENT AND RESPONSIBILITY: ESSAYS IN THE PHILOSOPHY OF LAW 180–83 (2008) (noting that the rule of law enables individuals "to predict and plan the future course of [their] lives within the coercive framework of the law. . . . to foresee the times of the law's interference"); FRIEDRICH A. HAYEK, THE ROAD TO SERFDOM 72 (1944) (recognizing that the rule of law "make[s] it possible to foresee with fair certainty how the [government] will use its coercive powers in given circumstances and to plan one's individual affairs on the basis of this knowledge."); Meir Dan-Cohen, *Decision Rules and Conduct Rules: On Acoustic Separation in Criminal Law*, 97 HARV. L. REV. 625, 670 (1984) ("By enhancing the individual's life-planning capacity, the rule of law expands freedom of action, secures a measure of individual liberty, and expresses respect for individual autonomy.").

324. *See, e.g.*, Tyler, *supra* note 316, at 1557 ("It is investigat[ive] stops that are key to mistrust since people feel they are uncontrollable. Obeying the law does not stop the police from stopping people on the street. And the behavior of officers is often reported to veer off of a professional script into actions that are humiliating and threatening.").

325. *See* PATRICK SHARKEY, STUCK IN PLACE: URBAN NEIGHBORHOODS AND THE END OF PROGRESS TOWARD RACIAL EQUALITY 114–17 (2013); Jeffrey Fagan & Elliott Ash, *New Policing, New Segregation: From Ferguson to New York*, 106 GEO. L.J. ONLINE 33, 100–04 (2017).

326. *See* JAMES FORMAN, JR., LOCKING UP OUR OWN: CRIME AND PUNISHMENT IN BLACK AMERICA 151–84 (2017) (describing the cumulative impact of aggressive and often unlawful policing in poor and minority communities); Fagan & Ash, *supra* note 325, at 104–18. Such negative effects include harm to the physical and mental health of residents. *See id.* at 122–24.

327. Richard A. Bierschbach & Stephanos Bibas, *Rationing Criminal Justice*, 116 MICH. L. REV. 187, 189 (2017).

IV. SKETCHING THE PATH AHEAD

Before *Utah v. Strieff*, police were aware that lawful securing of personal identity, such as by means of a valid Terry stop or voluntary disclosure, afforded access to a trove of valuable database information. After *Strieff*, they now know that they can secure such information unlawfully. Meanwhile, what was earlier referred to as the "identity exception" allows police to secure identity information unlawfully and match it to government database information without fear of the exclusionary rule being applied.[328]

The two doctrinal vectors, which originated and evolved independently of one another, share a key feature: they both fail to take account of the major strategic value of identity in modern day policing. It is past time for courts, including the Supreme Court, to take account of this critically important shift.

A. *CLEARING AWAY THE DOCTRINAL UNDERBRUSH*

For this to occur, it is first necessary to address several doctrinal misunderstandings. First and foremost, courts are wrong when they attach dispositive importance to the fact that database information accessed by police pre-exists the challenged police wrongdoing.[329] This is because the database information accessed in *Strieff*, *Tolentino* and similar cases is quintessential secondary, derivative evidence, the legal materiality of which became apparent to police only as a result of their misconduct (i.e., their unlawful demand of personal identity).[330] Much like the fingerprints unlawfully secured by police in *Davis v. Mississippi*, identity information in such cases is "something of evidentiary value which the public authorities have caused an arrested person to yield to them during illegal detention."[331] The evidentiary value lies in the role identity plays in linking an individual to information in a database.[332]

---

328. *See supra* Section II.B.

329. *See* Utah v. Strieff, 136 S. Ct. 2056, 2061 (2016) (deeming "discovery of a valid, pre-existing, and untainted arrest warrant" an intervening event that attenuated police misconduct); People v. Tolentino, 926 N.E.2d 1212, 1215 (N.Y. 2010) (finding determinative fact that "public records [are] already in the possession of authorities"); *see also, e.g.*, United States v. $493,850.00 in U.S. Currency, 518 F.3d 1159, 1165 (9th Cir. 2008) ("The information at issue here is not a fruit of the poisonous tree because it was not discovered subsequent to the illegal seizure . . . . [It] was learned from preexisting, unrelated investigations." (citations omitted)).

330. Aggravating matters, it can be difficult for individuals to establish standing to contest government access to databases. *See* 6 LAFAVE, *supra* note 133, § 11.4, at 325–26 & n.22 (citing courts taking the "erroneous approach" of requiring independent standing regarding government records accessed); United States v. Olivares-Rangel, 458 F.3d 1104, 1118 (10th Cir. 2006) (disagreeing with the view that standing exists "only when the defendant has standing regarding both the *violation* which constitutes the poisonous tree *and* separate standing regarding the *evidence* which constitutes the fruit of that poisonous tree").

331. Davis v. Mississippi, 394 U.S. 721, 724 (1969) (quoting Bynum v. United States, 262 F.2d 465, 467 (D.C. Cir. 1958)).

332. A critical point not diminished by the fact that police could have discovered individual identity by lawful means. *See id.* at 725 n.4 (stating that "the fact that equivalent evidence can

Importantly, moreover, language in *United States v. Crews*,[333] to the effect that the exclusionary rule "does not reach backward to taint information that was in official hands prior to any illegality,"[334] does not dictate to the contrary. In *Crews*, the evidence challenged—an in-court identification by a witness—had an independent, pre-existent factual basis, which "neither resulted from nor was biased by the unlawful police conduct."[335] The courtroom identification did not depend on the photo taken by police following Crews' unlawful arrest because police already knew the suspect's identity and were actively investigating him prior to his unlawful arrest.[336] The *Crews* Court expressly stated that "the Fourth Amendment violation in this case yielded nothing of evidentiary value that the police did not already have in their grasp."[337]

The police misconduct in *Strieff* and *Tolentino* differed critically from that in *Crews*. It most definitely provided what *Crews* referred to as something "of evidentiary value that the police did not already have in their grasp"[338]: knowledge of personal identity that "link[ed] together two extant ingredients in [the] identification"[339]—the individual unlawfully seized and the incriminating information (in *Strieff*, an arrest warrant) stored in a government database. Also, unlike in *Crews*, as well as in *United States v. Ceccolini*,[340] where a testifying witness was identified as the result of police

conveniently be obtained in a wholly proper way" does not suffice as a reason for not excluding the fruits of police misconduct because threatened exclusion seeks to make "those administering the criminal law understand that they must" obtain evidence legally (quoting *Bynum*, 262 F.2d at 468–69)).

333. United States v. Crews, 445 U.S. 463 (1980).

334. *Id.* at 475; *see also* Maryland v. Macon, 472 U.S. 463, 471 (1985) ("The exclusionary rule . . . does not reach backward to taint information that was in official hands prior to any illegality." (quoting *Crews*, 445 U.S. at 475)); Segura v. United States, 468 U.S. 796, 814 (1984) ("None of the information on which the warrant was secured was derived from or related in any way to the illegal entry into petitioners' apartment; the information came from sources wholly unconnected with the entry and was known well before the initial entry.").

335. *Crews*, 445 U.S. at 473.

336. *See id.* at 475 ("[T]he record plainly discloses that prior to his illegal arrest, the police both knew respondent's identity and had some basis to suspect his involvement in the very crimes with which has charged.").

337. *Id.*

338. *Id.*

339. *Id.*; *see also id.* at 475–76 (noting "*Davis* v. *Mississippi*, 394 U.S. 721 (1969), in which the defendant's identity and connection to the illicit activity were only first discovered through an illegal arrest or search," triggering suppression under the exclusionary rule); United States v. Olivares-Rangel, 458 F.3d 1104, 1120 (10th Cir. 2006) (suppressing "previously compiled Government records" when obtained through "exploitation of an illegal search and seizure [that] produced the critical link between a defendant's identity and his . . . criminal history record").

340. United States v. Ceccolini, 435 U.S. 268 (1978).

illegality,[341] *Tolentino* and *Strieff* involved databases—not witnesses whose autonomous exercise of free will dissipated taint.[342]

Nor should it matter whether the pre-existing data accessed was secured lawfully or unlawfully by police. Elsewhere, I have argued that police should not be able to retain unlawfully secured information, especially biometric information,[343] and continue to adhere to that position.[344] Indeed, allowing police to unlawfully seize an individual, unlawfully demand identity information, and access unlawfully secured information effectively countenances three constitutional wrongs.

The same should be said, however, of lawfully secured evidence. Professor Richard Re, in advocating a "due process exclusionary rule," urges a contrary position. According to Re, "what is lawfully learned at one time is lawfully learned forever, and the taint of a Fourth Amendment violation should never run backward in time."[345] Such a view gives short shrift to the powerful strategic incentive police have to access databases, including by

---

341. In *Ceccolini*, the Court upheld the admission of testimony by a store employee where the police learned of the employee's knowledge as a result of an inquiry following an illegal search of a drawer in the store. *Id.* at 269–70, 279–80.

342. *See* United States v. Akridge, 346 F.3d 618, 633–34 (6th Cir. 2003) (Moore, J., dissenting) (noting that of the several factors informing the Court's analysis in *Ceccolini* the exercise of free will by a witness was of paramount importance); *see also Ceccolini*, 435 U.S. at 277 (reasoning that "the illegality which led to the discovery of the witness very often will not play any meaningful part in the witness' willingness to testify").

343. *See* Logan, *supra* note 36, at 1604.

344. A position, it should be added, echoed by the Supreme Court in its foundational exclusionary rule decision *Silverthorne Lumber Co. v. United States,* 251 U.S. 385 (1920). In *Silverthorne*, federal agents, "without a shadow of authority," undertook "a clean sweep of all the books, papers[,] and documents found" in the office of Silverthorne and his father. *Id.* at 390. The trial court granted defendants' motion to suppress the materials, yet the government made copies and pursued an indictment "based upon the knowledge thus obtained." *Id.* at 390–91. The government subpoenaed the defendants to produce the originals, and defendants were held in contempt for refusing to comply. *Id.* at 391. The Supreme Court, in a 7-2 decision authored by Justice Holmes, flatly rejected the government's position:

> The proposition could not be presented more nakedly. It is that although of course its seizure was an outrage which the Government now regrets, it may study the papers before it returns them, copy them, and then may use the knowledge that it has gained to call upon the owners in a more regular form to produce them; that the protection of the Constitution covers the physical possession but notany advantages that the Government can gain over the object of its pursuit by doing the forbidden act.

Id.

345. Richard M. Re, *The Due Process Exclusionary Rule*, 127 HARV. L. REV. 1885, 1962 (2014). Re adds in a footnote without elaboration that "[t]his assumption may not always hold true: querying a database may sometimes constitute an independent search requiring its own justification, even if the database is in the government's possession." *Id.* at 1962 n.415. Re would, however, bar admission of the fruits of unlawful police action (e.g., the drugs found on Strieff when he was arrested and searched based on the discovered arrest warrant). *Id.* at 1962.

unlawful means as *Strieff* now permits.[346] It also underscores the need to develop new ways of conceiving of Fourth Amendment doctrine, as discussed next.

B. DOCTRINAL PATHS

With the foregoing clarified, discussion now turns to the affirmative case for regulating police wherewithal to unlawfully secure identity information and access government database information.

1. Fourth Amendment

The most important and obvious path entails re-conceptualizing scenarios such as presented in *Strieff* not as attenuation doctrine cases but rather as identity-data seizure cases. Such an approach would be based on the Court's treatment of "stop and identify" statutes, especially *Brown v. Texas*,[347] which overturned the conviction of a petitioner based on his refusal to comply with a state law that allowed police to demand the name and address of unlawfully detained individuals.[348] The unanimous Court noted at the outset that "[w]hen the officers detained appellant for the purpose of requiring him to identify himself, they performed a seizure of his person subject to the requirements of the Fourth Amendment."[349] Brown, like Strieff, was unlawfully seized simply for being in a place (an alley in a neighborhood frequented by drug users) that "looked suspicious."[350] The unlawful police seizure of Brown and demand that he provide identifying information without legal basis[351] created a "risk of arbitrary and abusive police practices [that] exceeds tolerable limits."[352]

Fifteen years later, in *Hiibel v. Sixth Judicial District Court of Nevada*, the Court upheld a conviction based on a Nevada law that criminalized refusal of lawfully detained individuals to provide identity information to police.[353] Hiibel, unlike Brown and Strieff, was lawfully seized by police.[354] In such a

346. *Cf.* United States v. Weikert, 504 F.3d 1, 16–17 (1st Cir. 2007) ("[I]t may be time to reexamine the proposition that an individual no longer has any expectation of privacy in information seized by the government so long as the government has obtained that information lawfully. . . . [T]here may be a persuasive argument . . . that an individual retains an expectation of privacy in the future uses of her DNA profile." (footnote omitted)).

347. Brown v. Texas, 443 U.S. 47, 52 (1979).

348. *Id.* at 49, 53.

349. *Id.* at 50.

350. *Id.* at 52 (quoting Officer Venegas, one of the arresting officers).

351. In a footnote, the Court emphasized that it "need not decide whether an individual may be punished for refusing to identify himself in the context of a lawful investigatory stop which satisfies Fourth Amendment requirements." *Id.* at 53 n.3. The latter question was resolved in *Hiibel v. Sixth Judicial Dist. Court*, 542 U.S. 177, 188–89 (2004).

352. *Brown*, 443 U.S. at 52.

353. *Hiibel*, 542 U.S. at 191.

354. *Id.* at 184.

situation, the Court properly recognized, police have a legitimate, administrative need to determine identity:

> Obtaining a suspect's name in the course of a Terry stop serves important government interests. Knowledge of identity may inform an officer that a suspect is wanted for another offense, or has a record of violence or mental disorder. . . . Identity may prove particularly important in cases such as this, where the police are investigating what appears to be a domestic assault. Officers called to investigate domestic disputes need to know whom they are dealing with in order to assess the situation, the threat to their own safety, and possible danger to the potential victim.[355]

Moreover, as the *Hiibel* majority noted, *Terry* itself does not allow a search or seizure in order to determine if the "suspect is wanted for another offense."[356]

In its most recent Term, the Court again evinced its concern over the constitutionality of police unlawfully securing identifying information. In *Collins v. Virginia*,[357] the Court by an eight-to-one vote held that police, who unlawfully entered the driveway of an individual suspected of possessing a stolen motorcycle, were not permitted to access license plate and vehicle identification numbers on the motorcycle that was hidden beneath a tarp.[358] The ability of police to view the motorcycle lawfully, from outside the curtilage, the Court reasoned, "certainly does not permit an officer physically to intrude on curtilage, remove a tarp to reveal license plate and vehicle

355. *Id.* at 186; *see also id.* at 187–88 ("The request for identity has an immediate relation to the purpose, rationale, and practical demands of a *Terry* stop. . . . A state law requiring a suspect to disclose his name in the course of a valid *Terry* stop is consistent with Fourth Amendment prohibitions against unreasonable searches and seizures."); *cf.* ACLU v. Clapper, 959 F. Supp. 2d 724, 734 (S.D.N.Y. 2013) (noting that federal agents must have "reasonable articulable suspicion" before conducting a NSA database query, adding that "[t]he . . . requirement ensures an 'ordered and controlled' query and prevents general data browsing" (quoting a declaration by Teresa H. Shea, the National Security Agency's Director of the Signals Intelligence Directorate)); State v. Dickey, 203 So. 3d 958, 961 (Fla. Dist. Ct. App. 2016) (noting that providing a false name to law enforcement is a crime only when "it occurs during a lawful detention or arrest"). Despite its lawfulness, question exists over the actual need of the officer in *Hiibel* to demand identifying information. As Justice Stevens noted in his dissent, to the extent the officer was concerned about risk of violence (Hiibel was detained on suspicion of assaulting his passenger), he could have but did not conduct a frisk for weapons. *Hiibel*, 542 U.S. at 196 n.7 (Stevens, J., dissenting). Moreover, as Professor Arnold Loewy pointed out, in the case "reasonable suspicion was predicated upon an alleged assault on a female. Having found Hiibel by the side of the road and a young woman in the truck, one would have thought that the first step would be to ascertain the well-being of the female, not the name of the male." Arnold H. Loewy, *The Cowboy and the Cop: The Saga of Dudley Hiibel, 9/11, and the Vanishing Fourth Amendment*, 109 PENN ST. L. REV. 929, 937 (2005).

356. *Hiibel*, 542 U.S. at 186.

357. Collins v. Virginia, 138 S. Ct. 1663 (2018).

358. *Id.* at 1670–71, 1675.

identification numbers, and use those numbers to confirm that the defendant committed a crime."[359]

In light of the foregoing, the officer in *Strieff* violated the Fourth Amendment in two respects—in conducting an unlawful seizure and in unlawfully demanding disclosure of personal identity. Worse yet, he leveraged the two constitutional wrongs to secure derivative evidence contained in a government database to arrest and search for evidence or contraband, which as discussed above should have been suppressed. By withholding application of the exclusionary rule, the *Strieff* Court flouted the premise that the rule should place the government in the same, not better, position it would have occupied absent the police misconduct in question.[360]

When police unlawfully secure and use identity information they do so to effectively de-anonymize individuals, defeating what Jeffrey Skopek has referred to as the reasonable "right to anonymity."[361] Government authority to defeat this right is predicated on the lawfulness of police conduct whereby identity is secured.[362] As Skopek notes,

> [t]he fact that this interest in anonymity can be outweighed by competing government interests—in [*Hiibel*], the same interests that allowed the police to temporarily seize the suspect for the Terry stop—does not diminish but rather reinforces the fact that it is an interest protected by the Fourth Amendment.[363]

Although Skopek's focus is on the Fourth Amendment exceptions for information secured by police as a result of public exposure (e.g., driving a car) and information possessed by third parties, his conceptual understanding has utility here. While often conflated, privacy and anonymity "differ in a fundamental and legally relevant way: Privacy hides the information, whereas anonymity hides what makes it personal."[364] What we should "expect to remain unknown," Skopek points out, "is the fact that this information is information about us,"[365] a distinct interest worthy of judicial

359. *Id.* at 1673 n.3.

360. *See* Arizona v. Evans, 514 U.S. 1, 19 (1995) (Stevens, J., dissenting) (citing Potter Stewart, *The Road to* Mapp v. Ohio *and Beyond: The Origins, Development and Future of the Exclusionary Rule in Search-and-Seizure Cases*, 83 COLUM. L. REV. 1365, 1392 (1983)).

361. Jeffrey M. Skopek, *Reasonable Expectations of Anonymity*, 101 VA. L. REV. 691, 725 n.119 (2015); *see also id.* at 718–19 ("[A]nonymity and privacy refer to conditions that are created by the same event: splitting a person's identity and a piece of information about that person.").

362. *Id.* at 727–28 (noting that "the Court held that compelled identification was only constitutional in 'the course of a valid *Terry* stop'" and that "the Court recognized that the Fourth Amendment protects a suspect's interest in remaining anonymous" (quoting *Hiibel*, 542 U.S. at 188)); *see also* Maryland v. King, 569 U.S. 435, 463 (2013) (holding that government has an interest in securing DNA sample for lawfully arrested individual to confirm personal identity).

363. *See* Skopek, *supra* note 361, at 728 (footnote omitted).

364. *Id.* at 761.

365. *Id.* at 762.

recognition and protection.[366] It is the same interest that the Supreme Court elsewhere has referred to as the interest in "practical obscurity,"[367] which is no less worthy of protection simply because one's physical identity is revealed as the result of electing to be in public.[368]

Constraining police authority to de-anonymize individuals comes at a cost, however, one highlighted by debates among some privacy law scholars who assert that the social benefits of transparency outweigh individual interests in nondisclosure. Society, in Diane Zimmerman's words, "has a powerful countervailing interest in exchanges of accurate information about the private lives and characters of its citizen[s]."[369] From a wealth maximization standpoint, as Seth Kreimer put it, "[a]s knowledge increases so does societal and individual freedom. . . . Those who suppress information may be seeking to manipulate an audience's choices."[370]

Whatever the merits of such arguments in the abstract, they have worrisome consequences in the law enforcement context. This is because police officers are distinct from other members of society, such as employers interested in the criminal history information of prospective employees.[371]

366. *See id.* ("[F]or our law to adequately respond to the emergence of big data practices that collect, store, and aggregate . . . information, we need to be thinking in terms of anonymity as well as privacy. It is only in this way that we will be able to recognize and protect the important legal interests that are implicated by these new threats to the secrecy of our personal information."). For similar arguments regarding what might be termed a right to anonymity, see generally Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 MISS. L.J. 213 (2002) (discussing the Fourth Amendment's role in regulating surveillance cameras). The right is also extensively discussed in the non-legal literature. *See generally, e.g.*, Gary T. Marx, *What's in a Name? Some Reflections on the Sociology of Anonymity*, 15 INFO. SOC'Y 99 (1999) (discussing the ramifications of the increasing technological capability to reduce anonymity and achieve "identifiability").

367. U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 780 (1989) (holding that the Freedom of Information Act does not require disclosure of "rap sheets"). The right has likewise been vigorously protected by the Court in cases involving efforts to compel information regarding membership in political and civic organizations. *See supra* note 320 and accompanying text.

368. *Cf.* Watchtower Bible & Tract Soc'y of N.Y., Inc. v. Vill. of Stratton, 536 U.S. 150, 167 (2002) ("The fact that [religious canvassers] revealed their physical identities did not foreclose our consideration of the [canvassers'] interest in maintaining their anonymity.").

369. Diane L. Zimmerman, *Requiem for a Heavyweight: A Farewell to Warren and Brandeis's Privacy Tort*, 68 CORNELL L. REV. 291, 341 (1983); *see also* RICHARD A. POSNER, ECONOMIC ANALYSIS OF LAW § 3.3, at 51–52, § 23.2, at 845–47 (8th ed. 2011) (assessing the economic efficiency implications of individuals' hiding personal information).

370. Seth F. Kreimer, *Sunlight, Secrets, and Scarlet Letters: The Tension Between Privacy and Disclosure in Constitutional Law*, 140 U. PA. L. REV. 1, 72 (1991); *see also* Richard A. Epstein, *The Legal Regulation of Genetic Discrimination: Old Responses to New Technology*, 74 B.U. L. REV. 1, 12 (1994) ("[T]he plea for privacy is often a plea for the right to misrepresent one's self to the rest of the world.").

371. *See, e.g.*, Lior Jacob Strahilevitz, *Privacy Versus Antidiscrimination*, 75 U. CHI. L. REV. 363, 365 (2008). As reasons supporting recent efforts to "ban the box" in hiring decisions attest, however, the criminal history criterion in initial job screening decisions can be both unfair and a misleading proxy for assessing employee quality and reliability. CHRISTINA STACY & MYCHAL COHEN, URBAN INST., BAN THE BOX AND RACIAL DISCRIMINATION: A REVIEW OF THE EVIDENCE AND

Indeed, this is a chief reason why the Fourth Amendment regulates information secured by police, but not private parties; it is the police who enjoy the government-conferred monopoly to invade the privacy and bodily security of individuals.[372] Moreover, the market model is premised on the availability of accurate information, which as noted earlier is not always the case with criminal justice databases.[373]

In short, *Strieff* was not only wrong on the doctrinal merits, but it was wrong in the way it framed the issue before the Court. By failing to regard unlawful police acquisition of identity information as a distinct Fourth Amendment event, the Court missed a critical analytic step in its exclusionary rule analysis. Viewing the *Strieff* facts in such a light will require a new way of conceiving Fourth Amendment doctrine, one that is better attuned to the realities of database policing. Multiple scholars have of late argued that technological advances require a reconceptualization of Fourth Amendment doctrine more generally,[374] and recent decisions from the Court evince an awareness of the need for change.[375] Just as the third party doctrine, which has historically deemed information held by third parties as beyond the reach of Fourth Amendment protection,[376] is now being questioned as a result of enhanced police wherewithal to collect and store data,[377] doctrine allowing police to unlawfully demand personal identifiers and access information must be reexamined.[378]

POLICY RECOMMENDATIONS 1–5 (2017), https://www.urban.org/sites/default/files/publication/88366/ban_the_box_and_racial_discrimination.pdf.

372. Burdeau v. McDowell, 256 U.S. 465, 475 (1921) (stating that the origin and history of the Fourth Amendment demonstrates an intent to limit only the activities of governmental agents).

373. *See supra* Part III.

374. *See, e.g.*, Margaret Hu, *Biometric ID Cybersurveillance*, 88 IND. L.J. 1475, 1556 (2013) (asserting that Fourth Amendment doctrine must evolve in light of new "identity management systems and bureaucratized cybersurveillance"); Joh, *supra* note 14, at 38 (asserting "the need to draw new Fourth Amendment lines now that the government has the capability and desire to collect and manipulate large amounts of digitized information").

375. *See, e.g.*, Riley v. California, 134 S. Ct. 2473, 2489 (2014) (requiring a warrant for cell phone searches and noting that "[o]ne of the most notable distinguishing features of modern cell phones is their immense storage capacity. Before cell phones, a search of a person was limited by physical realities and tended as a general matter to constitute only a narrow intrusion on privacy."); *cf.* U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 764 (1989) (noting that "there is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information"); Katz v. United States, 389 U.S. 347, 352 (1967) (noting in its Fourth Amendment analysis "the vital role that the public telephone has come to play in private communication").

376. *See generally* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561 (2009) (defending the third-party Fourth Amendment doctrine).

377. *See, e.g.*, United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring) (opining that "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties").

378. *See* Erin Murphy, *Databases, Doctrine & Constitutional Criminal Procedure*, 37 FORDHAM URB. L.J. 803, 826 (2010) (urging attention to "ways in which databases represent a new form of

2. Fifth Amendment

Demanding and securing personal identity information can also implicate the Fifth Amendment's privilege against compelled self-incrimination.[379] The Court in *Hiibel* assumed that "[s]tating one's name may qualify as an assertion of fact relating to identity," and that "[p]roduction of identity documents might meet the definition as well,"[380] satisfying the Fifth Amendment requirement that words or action be "testimonial."[381] To the five-member majority, however, Hiibel was unable to establish that disclosure of his identity would result in potential criminal liability, "or that it 'would furnish a link in the chain of evidence needed to prosecute.'"[382] Rather, Hiibel refused to self-identify "because he thought his name was none of the officer's business."[383] While the majority left open the possibility whether the Fifth Amendment would protect compelled disclosure of identity, it opined that being compelled

> to disclose a name is likely to be so insignificant in the scheme of things as to be incriminating only in unusual circumstances. . . . Still, a case may arise where there is a substantial allegation that furnishing identity at the time of a stop would have given the police a link in the chain of evidence needed to convict the individual of a separate offense.[384]

The two dissenting opinions in *Hiibel*, by Justices Stevens and Breyer, singled out the Fifth Amendment ramifications of the majority's decision for special concern. Justice Stevens, writing alone, reasoned that forcing disclosure of personal identity was both testimonial and incriminating: "why else," he asked, would an officer demand it, and "the Nevada Legislature [statutorily] require . . . disclosure . . . when circumstances 'reasonably indicate that the person has committed, is committing or is about to commit a crime'?"[385] Of particular importance to the discussion here, Justice Stevens added that even if a name is not in itself inculpatory, it

---

collection, use, and dissemination of information" but omitting attention to identity acquisition and database access); *see also* Arizona v. Evans, 514 U.S. 1, 17 (1994) (O'Connor, J., concurring) (expressing concern over "the advent of powerful, computer-based recordkeeping systems that facilitate arrests in ways that have never before been possible"); LAWRENCE LESSIG, CODE VERSION 2.0, at 202–03 (2006) (differentiating monitoring behavior from making it searchable and asserting that "[d]igital technologies change this balance—radically").

379. U.S. CONST. amend. V ("No person . . . shall be compelled in any criminal case to be a witness against himself . . . .").

380. Hiibel v. Sixth Judicial Dist. Court, 542 U.S. 177, 189 (2004).

381. *Id.*

382. *Id.* at 190 (quoting Hoffman v. United States, 341 U.S. 479, 486 (1951)).

383. *Id.*

384. *Id.* at 191.

385. *Id.* at 196 (Stevens, J., dissenting) (quoting NEV. REV. STAT. § 171.123(1) (2003)).

> can provide the key to a broad array of information about the person, particularly in the hands of . . . police officer[s] with access to a range of law enforcement databases. And that information, in turn, can be tremendously useful in a criminal prosecution. It is therefore quite wrong to suggest that a person's identity provides a link in the chain to incriminating evidence "only in unusual circumstances."[386]

Justice Breyer in his dissent (joined by Justices Souter and Ginsburg), likewise recognized the incriminating consequences possibly flowing from compelled disclosure of personal identity. According to Justice Breyer, "a name itself—even if it is not 'Killer Bill' or 'Rough 'em up Harry'—will sometimes provide the police with 'a link in the chain of evidence needed to convict the individual of a separate offense.'"[387]

After *Hiibel*, several scholars elaborated upon the dissents' concerns. Michael Pardo and Daniel Steinbock, for instance, noted that identity can serve as a link to an arrest warrant in a database,[388] as later occurred in *Strieff*. Given the enormous volume of outstanding arrest warrants in databases (valid or invalid), the odds are quite high indeed—not "unusual" as the *Hiibel* majority speculated—that a warrant exists.[389] Even more problematic, the officer in *Strieff* demanded and received not only Strieff's name but also identity documentation,[390] a matter of critical importance because as Professor Wayne LaFave observes the latter "is likely to provide the officer with information about the person above and beyond identity" that can dramatically expand data matching,[391] a major development ignored by the *Strieff* Court.

---

386. *Id.* (quoting majority opinion).

387. *Id.* at 199 (Breyer, J., dissenting) (quoting majority opinion).

388. Michael S. Pardo, *Disentangling the Fourth Amendment and the Self-Incrimination Clause*, 90 IOWA L. REV. 1857, 1895 (2005); Daniel J. Steinbock, *National Identity Cards: Fourth and Fifth Amendment Issues*, 56 FLA. L. REV. 697, 718 (2004).

389. *See Hiibel*, 542 U.S. at 191.

390. *See supra* note 23 and accompanying text. In *Hiibel*, the Court emphasized that the Nevada law challenged,

> [a]s we understand it, . . . does not require a suspect to give the officer a driver's license or any other document. Provided that the suspect either states his name or communicates it to the officer by other means—a choice, we assume, that the suspect may make—the statute is satisfied and no violation occurs.

Hiibel, 542 U.S. at 185. According to the transcript of the dialog between Hiibel and the arresting officer, however, the officer repeatedly demanded to "see some identification" and "show me your identification." Loewy, *supra* note 355, at 931–33 (quoting arresting officer Deputy Sheriff Lee Dove).

391. 6 LAFAVE, *supra* note 133, § 9.6(g).

3. Remedy

Simply concluding that unlawfully secured identifying information qualifies as a constitutional wrong, however, leaves a key question unresolved: does the wrong always trigger application of the exclusionary rule? With the Fifth Amendment, as the *Hiibel* Court observed, analysis turns on whether the individual has been forced to provide "police a link in the chain of evidence needed to convict the individual of a separate offense."[392]

With the Fourth Amendment, the answer similarly depends on the nature of the information accessed. With an arrest warrant, the answer is clear. When police discover that an individual is the subject of an arrest warrant, the individual is subject to arrest. Like defendant Lopez-Mendoza in the Supreme Court case of the same name, the individual cannot be heard to argue that the justice system lacks jurisdiction over his body.[393] By extension, Strieff was subject to arrest and being held to account in court as a jurisdictional matter. As the Court said of Lopez-Mendoza, in the context of an immigration violation, "[w]hen the crime in question involves unlawful presence in this country, the criminal may go free, but he should not go free within our borders."[394]

Whether evidence or contraband discovered in a search incident to such an arrest should be admissible, however, is another matter. This was what the Court addressed in *Strieff*, which, as discussed earlier, the Court got wrong.[395] Honoring the lawful arrest warrant as a jurisdictional matter aligns with rule of law concerns.[396] Allowing police use of evidence secured as a result of a

392. *Hiibel*, 542 U.S. at 191.

393. *See* I.N.S. v. Lopez-Mendoza, 468 U.S. 1032, 1039 (1984) ("The 'body' or identity of a defendant or [a] respondent in a criminal or civil proceeding is never itself suppressible as a fruit of an unlawful arrest, even if it is conceded that an unlawful arrest, search, or interrogation occurred.").

394. *Id.* at 1047; *see also* Frisbie v. Collins, 342 U.S. 519, 522 (1952) ("[T]he power of a court to try a person for [a] crime is not impaired by the fact that he had been brought within the court's jurisdiction by reason[s] of a 'forcible abduction.'").

395. *See supra* Sections II.A & IV.B.1.

396. This is not to say, however, that jurisdictions should not take steps to reduce their number of bench warrants for menial offenses and what one commentator recently referred to as "non-compliance" (e.g., failure to appear). Nirej Sekhon, *Dangerous Warrants*, 93 WASH. L. REV. 967, 969–71 (2018). Such warrants are not, contrary to the contention of the *Strieff* majority, "ministerial": police have substantial discretion to enforce them, as they are not enforcement priorities, and usually lie inert in databases until discovered by police. *Id.* at 971, 986 (quoting Utah v. Strieff, 136 S. Ct. 2056, 2063 (2016)). Steps should be undertaken to reduce the number of such warrants, as is now occurring in several jurisdictions. *See id.* at 1014–16. In conjunction with such efforts, consideration might be given to establishing a hierarchy of arrest warrants, requiring that police first issue a warning before arresting on the basis of an arrest warrant for non-serious offenses such as in *Strieff*, and arrest only if the individual does not resolve the warrant in a prescribed period of time. *See* Chanae L. Wood, Comment, *Black and Poor: The Grave Consequences of* Utah v. Strieff, 30 ST. THOMAS L. REV. 68, 90–91 (2017); *id.* at 90 n.140 (noting that very often individuals are unaware that a bench warrant has been issued for their arrest); *see also, e.g.*, Sekhon, *supra*, at 1010–16 (offering several strategies, including adoption by police departments of policies that eschew enforcement of non-compliance warrants).

search incident to arrest, however, does just the opposite: it encourages fishing expeditions—unlawful seizures undertaken to land bigger "fish" (i.e., discovering evidence of more serious criminal activity).[397] Aggravating matters, as the facts of *Strieff* make clear,[398] defendants face considerable difficulty in amassing evidence sufficient to establish "flagrant" misconduct by police,[399] or evidence that unlawful seizure "was part of any systemic or recurrent police misconduct."[400]

As noted in Part III, however, arrest warrants are only one kind of record contained in government databases. Another concerns what might be termed "investigative" information—for instance, records regarding past stops and arrests and biometric information. Here, the exclusionary rule is likewise needed to deter police misconduct.[401] As the Justices noted in the *Tolentino* oral argument, knowledge of individual identity can play a crucial role in police investigative efforts.[402] Again, suppressing an identifier and the information it reveals does not "put the police in a worse position than they would have been in absent any error or violation."[403] It simply precludes them from exploiting their misconduct to secure an investigative windfall. Discouraging police fishing expeditions will also decrease the incidence of

397. *See* United States v. Gross, 662 F.3d 393, 404 (6th Cir. 2011) (expressing concern, pre-*Strieff*, that withholding exclusionary rule will "create . . . a new form of police investigation, whereby an officer patrolling a high crime area may, without consequence, illegally stop a group of residents where he has a 'police hunch' that the residents may . . . have outstanding warrants"); *cf.* City of Indianapolis v. Edmond, 531 U.S. 32, 44 (2000) (noting concern that "stops justified only by the generalized and ever-present possibility that interrogation and inspection may reveal that any given motorist has committed some crime").

398. The *Strieff* majority considered the officer's misconduct "at most negligent." *Strieff*, 136 S. Ct. at 2063. The dissent characterized the officer's behavior quite differently. *See id.* at 2072 (Kagan, J., dissenting) (asserting that the seizure "was a calculated decision, taken with so little justification that the State has never tried to defend its legality"). Indeed, Officer Fackrell, who was investigating an anonymous tip of unknown reliability, candidly admitted that he lacked a legal basis to stop Strieff, and hoped "to 'find out what was going on [in] the house'" Strieff had exited. *Id.* at 2059, 2063 (majority opinion) (alteration in original) (quoting Officer Fackrell).

399. *See* Rebecca Laitman, Note, *Fourth Amendment Flagrancy: What It Is, and What It Is Not*, 45 FORDHAM URB. L.J. 799, 801 (2018) (noting ambiguity in the Court's definition of flagrant misconduct and difficulty in establishing its existence).

400. *Strieff*, 136 S. Ct. at 2063. In this regard, the majority's refusal to attach importance to data from Ferguson, Missouri, and elsewhere highlighting the common practice of police to conduct suspicionless stops to check for warrants, noted by Justice Sotomayor in dissent, underscores the difficulty of establishing a case of "systematic or recurrent police misconduct." *Id.* at 2068 (Sotomayor, J., dissenting) (quoting majority opinion).

401. *See* Elkins v. United States, 364 U.S. 206, 217 (1960) ("The [exclusionary] rule is calculated to prevent, not to repair. Its purpose is to deter—to compel respect for the constitutional guaranty in the only effectively available way—by removing the incentive to disregard it.").

402. *See supra* notes 149–51 and accompanying text.

403. Murray v. United States, 487 U.S. 533, 537 (1988) (quoting Nix v. Williams, 467 U.S. 431, 443 (1984)).

non-legal harms, such as when police access embarrassing or personally sensitive information stored in government databases.[404]

Finally, application of the exclusionary rule is important because of the lack of alternate remedies. In *Strieff* and other recent cases, the Court has cited the availability of civil rights actions as a reason to withhold application of the exclusionary rule.[405] Securing relief in such actions, however, is very difficult for several reasons. First, unlawful stop cases turn on factual-legal determinations of reasonable suspicion, as to which courts show considerable deference to police in the field.[406] Second, in suits seeking monetary damages, officers can raise a qualified immunity defense, which "protect[s] . . . all but the plainly incompetent or those who knowingly violate the law."[407] The defense itself will often align with the most important factor in attenuation doctrine analysis: "the purpose and flagrancy of the official misconduct,"[408] meaning that a civil rights remedy will only be available when the exclusionary rule also applies.

Civil rights cases also face two other major practical difficulties. The first is that if the exclusionary rule is not applied and evidence is admitted, the targeted individual will be more likely to plead guilty, including to a lesser charge, making it even more difficult to prevail on a Section 1983 false arrest claim.[409] The second is that very often individuals unlawfully detained, yet not prosecuted because police discover no evidence of wrongdoing, do not file civil actions.[410]

C. STATUTORY FIX

Of late, it has become common to hear advocacy in favor of legislative (as opposed to judicial-constitutional) limits on police authority. Professor Orin Kerr, for instance, points to the relative superior institutional capacity of legislatures to gather facts, weigh expert testimony, and respond to

404. *See supra* notes 271–86 and accompanying text.

405. *See* Utah v. Strieff, 136 S. Ct. 2056, 2064 (2016); Hudson v. Michigan, 547 U.S. 586, 597 (2006).

406. Anna Lvovsky, *The Judicial Presumption of Police Expertise*, 130 HARV. L. REV. 1995, 2052–56 (2017).

407. Malley v. Briggs, 475 U.S. 335, 341 (1986).

408. *See Strieff*, 136 S. Ct. at 2062 (quoting Brown v. Illinois, 422 U.S. 590, 604 (1975)).

409. *See* Katherine A. Macfarlane, *Predicting* Utah v. Streiff's *Civil Rights Impact*, 126 YALE L.J.F. 139, 143–45 (2016).

410. *See* Oren Bar-Gill & Barry Friedman, *Taking Warrants Seriously*, 106 NW. U. L. REV. 1609, 1628–32 (2012) (citing reasons explaining why aggrieved individuals are reluctant to file suit); Macfarlane, *supra* note 409, at 143–47 (noting similar factors that lessen the likelihood that counsel will take action on such cases, including how settlements can limit or negate recovery of statutory attorney fees). On the point that Fourth Amendment doctrine more generally fails to afford redress to the many individuals searched and seized, and no evidence or contraband is found, see Tonja Jacobi & Ross Berlin, *Supreme Irrelevance: The Court's Abdication in Criminal Procedure Jurisprudence*, 51 U.C. DAVIS L. REV. 2033, 2063–66 (2018).

technological change, while maintaining democratic accountability.[411] More recently, Justice Alito in *United States v. Jones* voiced optimism over the prospect for legislative intervention noting, inter alia, congressional limits in the late 1960s imposed on police wiretapping.[412]

A legislative provision could be enacted that would deny police the authority to demand personal identity information absent a lawful investigative stop or arrest,[413] and require suppression of evidence that was secured as a result,[414] subject to the exceptions discussed. And because the limit would be predicated on Fourth Amendment reasonableness principles—i.e., police demanding identification based on a constitutionally lawful seizure—the Supreme Court presumably would lack basis to second-guess the limit on constitutional grounds, as it did in *Virginia v. Moore*.[415] Likewise, in line with the preceding discussion regarding the Fifth Amendment, a jurisdiction could legislatively proscribe unlawfully compelled identity information that is incriminating.[416]

Experience suggests, however, that such an intervention is not likely to materialize. Most important, well-known public choice/political process factors militate against adoption of laws possibly regarded as pro-criminal defendant.[417] Strieff, for instance, had a valid arrest warrant out for him

411. Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 857–87 (2004).

412. United States v. Jones, 565 U.S. 400, 426–27 (2012) (Alito, J., concurring); *see also* Riley v. California, 134 S. Ct. 2473, 2497–98 (2014) (Alito, J., concurring) (regarding it preferable for Congress or state legislatures to regulate police searches of cell phones).

413. An example of what Professor John Rappaport has referred to as "second-order regulation" of law enforcement, whereby a legislatively enacted rule implements a constitutionally based value. John Rappaport, *Second-Order Regulation of Law Enforcement*, 103 CALIF. L. REV. 205, 231–45 (2015).

414. *See* George E. Dix, *Nonconstitutional Exclusionary Rules in Criminal Procedure*, 27 AM. CRIM. L. REV. 53, 63–66 (1989) (discussing reluctance of courts to exclude evidence in absence of statutory direction). In some instances, such as when biometric identity information is secured, the materials should be destroyed, contrary to common current practice. *See* Logan, *supra* note 241, at 279–83.

415. Virginia v. Moore, 553 U.S. 164, 168–75 (2008). In *Moore*, a unanimous Court refused to suppress evidence secured as the result of an arrest that violated a Virginia statute limiting police authority to arrest for minor offenses reasoning that the search incident to arrest exception applied to "lawful arrest[s]," which require only probable cause, which was present. *Id.* at 176–77. The Court also deemed it significant that Virginia did not statutorily require exclusion of evidence secured by the search, reasoning that any requirement by the Court that suppression was required would trammel state prerogative. *Id.* at 174.

416. *Cf.* Thomas P. Sullivan & Andrew W. Vail, *The Consequences of Law Enforcement Officials' Failure to Record Custodial Interviews as Required by Law*, 99 J. CRIM. L. & CRIMINOLOGY 215, 218–23 (2008) (discussing legislative exclusionary rules triggered by failure to record interrogations).

417. *See generally* William J. Stuntz, *The Pathological Politics of Criminal Law*, 100 MICH. L. REV. 505 (2001) (describing the unique political dynamic driving harsh criminal justice legislation); *see also* Ronald F. Wright & Wayne A. Logan, *The Political Economy of Application Fees for Indigent Criminal Defense*, 47 WM. & MARY L. REV. 2045, 2046–49 (2006) (discussing relative lack of political influence of those typically targeted by the criminal justice system).

resulting in what the Court called the "ministerial act" of his arrest.[418] He was thus a scofflaw (albeit based on his failure to appear in court to resolve a minor traffic matter) and, worse yet, possessed drugs.[419] Moreover, as is commonly the case with criminal justice policy making, the issue could well lack political salience given that those most often adversely impacted lack political voice and influence.[420]

Legislative action, moreover, would likely face stiff resistance from law enforcement. Evidence of this influence is found in the multiple federal laws regulating the acquisition, accessing, and release of information, which consistently single out law enforcement agencies for exemption.[421] To Professor Erin Murphy, the author of the study revealing this exceptionalism, the cause was readily apparent: the political lobbying and influence of law enforcement interests who feared that their authority would be limited.[422] The Computer Matching Act and Privacy Protection Act of 1988 provides another example.[423] The Act limits government use of matching results under certain circumstances for the purpose of determining eligibility for federal program benefits or recovering money under such programs.[424] In particular, it prevents the government from taking adverse action before the data producing a match is verified and requires notice and an opportunity to be heard to challenge the match.[425] Tellingly, however, Congress included an

418. Utah v. Strieff, 136 S. Ct. 2056, 2063 (2016).

419. *Id.* at 2060.

420. *See generally, e.g.*, Donald A. Dripps, *Criminal Procedure, Footnote Four, and the Theory of Public Choice; Or, Why Don't Legislatures Give a Damn About the Rights of the Accused?*, 44 SYRACUSE L. REV. 1079 (1993) (discussing the various public choice and political process reasons behind harsh criminal justice policies); David M. Jaros, *Preempting the Police*, 55 B.C. L. REV. 1149, 1173 (2014) ("[P]oor urban minority communities, which experience a disproportionate share of police activity and are more likely to encounter questionable police practices, often have little political influence and lack the means to press legislators to openly debate issues." (footnote omitted)). For discussion of how political voicelessness plays out in the local criminal justice policy-making arena in particular, see Wayne A. Logan, *Fourth Amendment Localism*, 93 IND. L.J. 369, 384–86 (2018).

421. *See* Erin Murphy, *The Politics of Privacy in the Criminal Justice System: Information Disclosure, the Fourth Amendment, and Statutory Law Enforcement Exemptions*, 111 MICH. L. REV. 485, 487 (2013) ("The United States Code currently contains over twenty separate statutes that restrict both the acquisition and release of covered information. . . . Yet across this remarkable diversity, there is one feature that all these statutes share in common: each contains a provision exempting law enforcement from its general terms." (footnote omitted)).

422. *Id.* at 504 ("This heedfulness to the needs of law enforcement does not occur spontaneously. Instead, unsurprisingly, law enforcement representatives regularly and routinely weigh in to address the impact that statutory protections will have on their interests . . . .").

423. Computer Matching and Privacy Protection Act of 1988, 5 U.S.C. § 552a (2012).

424. *Id.*

425. *Id.* § 552a(p).

exception for law enforcement,[426] as it has done with the Freedom of Information Act regarding, *inter alia*, investigative techniques.[427]

In short, as with other criminal justice policy matters, little reason exists to think that Congress or state legislatures will act, necessitating action on the constitutional front.

V. CONCLUSION

Today, it is widely acknowledged that the constitutional regulation of police has not kept pace with the massive changes wrought by technological innovation. To a greater extent than ever before, police can collect, store and quickly access information regarding individuals, affording them enormous strategic benefit on street patrol. This benefit, however, can come at significant cost to individuals and their communities.

To date, courts and scholars have focused mainly on the collection and use of data, which while of critical importance only partly addresses the many problems presented by database policing. This article has shifted focus, addressing the need to better regulate police wherewithal to demand identity information, which allows them to access the expansive databases at their disposal, and offers suggestions for how this can be achieved.

The need for intervention is real and growing by the day. Already, police enjoy significant authority to secure personal identity information lawfully, such as when it is consensually provided or when they seize an individual based on the modest proof requirement of reasonable suspicion or probable cause. Soon, as well, they likely will be able to identify individuals by means of "remote biometric identifiers" that do not require physical seizures and demands for identification,[428] which should be but has yet to be subject to

426. Under the Act, limits do not apply to:

> matches performed, by an agency (or component thereof) which performs as its principal function any activity pertaining to the enforcement of criminal laws, subsequent to the initiation of a specific criminal or civil law enforcement investigation of a named person or persons for the purpose of gathering evidence against such person or persons . . . .

Id. § 552a(a)(8)(B)(iii).

427. *See generally* Stephen Wm. Smith, *Policing Hoover's Ghost: The Privilege for Law Enforcement Techniques*, 54 AM. CRIM. L. REV. 233 (2017) (discussing exemptions contained in federal Freedom of Information Act as well as in several state law analogs).

428. *See* Robinson Meyer, *Long-Range Iris Scanning Is Here,* ATLANTIC (May 13, 2015), https://www.theatlantic.com/technology/archive/2015/05/long-range-iris-scanning-is-here/393065; Kaveh Waddell, *Half of American Adults Are in Police Facial Recognition Databases*, ATLANTIC (Oct. 19, 2016), https://www.theatlantic.com/technology/archive/2016/10/half-of-american-adults-are-in-police-facial-recognition-databases/504560. Vehicle license plate readers, which while not as individualized because the person driving might not be the subject of an arrest warrant or other basis for a stop, provide another way for police to discern identity without need for a physical seizure and demand for identity. *See Street-Level Surveillance: Automated License Plate Readers (ALPRs)*, ELEC. FRONTIER FOUND., https://www.eff.org/pages/automated-license-plate-readers-alpr (last visited Oct. 24, 2018).

legal regulation.[429] More troubling still, in *Utah v. Strieff* the majority ominously stated that it felt "no need to decide whether the [arrest] warrant's existence alone would make the initial stop constitutional even if [the officer who unlawfully seized Strieff] was unaware of its existence."[430] In light of these realities, conceiving of unlawful police acquisition of personal identifying information as worthy of constitutional regulation becomes all the more important.

429. *See* Laura K. Donohue, *Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age*, 97 MINN. L. REV. 407, 463–504 (2012); Mariko Hirose, *Privacy in Public Spaces: The Reasonable Expectation of Privacy Against the Dragnet Use of Facial Recognition Technology*, 49 CONN. L. REV. 1591, 1615 (2017); *Biometric Identifiers*, ELEC. PRIVACY INFO. CTR., https://epic.org/privacy/biometrics (last visited Oct. 24, 2018).

430. Utah v. Strieff, 136 S. Ct. 2056, 2062 (2016).