# DITCHING "DNA ON DEMAND": A HARMS-CENTERED APPROACH TO SAFEGUARDING PRIVACY INTERESTS AGAINST DNA COLLECTION AND USE BY LAW ENFORCEMENT

## INTRODUCTION

In February 2022, news broke that the San Francisco Police Department had used a woman's DNA collected years prior—as part of a rape examination—to arrest her for retail theft.[1] In the wake of this revelation, the city's district attorney,[2] state and local politicians,[3] advocacy groups,[4] and the police chief himself,[5] all swiftly and forcefully denounced the practice of using DNA collected from sexual assault victims in subsequent, unrelated criminal investigations. Given the invasive nature of rape examinations and the already low reporting rates of sexual assaults to police,[6] the prompt condemnation of using a rape victim's DNA to investigate them for a later crime is perhaps unsurprising. And yet, by the time the news story broke, the San Francisco Police Department's practice

1. *See, e.g.*, Azi Paybarah, *Victim's Rape Kit Was Used to Identify Her as a Suspect in Another Case*, N.Y. TIMES (Feb. 15, 2022), https://www.nytimes.com/2022/02/15/us/san-francisco-police-rape-kit-dna.html [https://perma.cc/X37S-DBSU]; Eduardo Medina, *Woman Sues San Francisco over Arrest Based on DNA from Her Rape Kit*, N.Y. TIMES (Sept. 14, 2022), https://www.nytimes.com/2022/09/13/us/rape-kit-dna-san-francisco.html [https://perma.cc/W976-6CGK].

2. *See* Press Release, Chesa Boudin, District Attorney of San Francisco, DA Boudin Denounces Practice of Violating Rape Victim's Privacy and Misusing Sexual Assault DNA Evidence (Feb. 14, 2022), https://www.sfdistrictattorney.org/archive-press-release/da-boudin-denounces-practice-of-violating-rape-victims-privacy-and-misusing-sexual-assault-dna-evidence/ [https://perma.cc/8EWL-JQRM] (describing the practice of using rape victims' DNA to attempt to subsequently incriminate them as "legally and ethically wrong").

3. *See, e.g.*, *Senator Wiener Announces He Will Sponsor Legislation to Protect Rape Victims' DNA*, DAVIS VANGUARD (Mar. 7, 2022), https://www.davisvanguard.org/2022/03/senator-wiener-announces-he-will-sponsor-legislation-to-protect-rape-victims-dna/ [https://perma.cc/KVT4-LGC7] ("It's unacceptable to use survivors' DNA—given expressly for the purpose of finding or prosecuting a perpetrator—to incriminate that same survivor.").

4. *See* Press Release, RAINN, RAINN Responds to Law Enforcement Improperly Using a Survivor's DNA from Her Rape Kit (Feb. 15, 2022), https://www.rainn.org/news/rainn-responds-law-enforcement-improperly-using-survivor%E2%80%99s-dna-her-rape-kit [https://perma.cc/E5HE-AP4L] (describing storage of rape survivors' DNA in a database and use of DNA for any purpose other than identifying the perpetrator as "indefensible").

5. Chief William Scott of the San Francisco Police Department stated: "If it's true that DNA collected from a rape or sexual assault victim has been used by S.F.P.D. to identify and apprehend that person as a suspect in another crime, I'm committed to ending the practice." Paybarah, *supra* note 1.

6. More than two out of three sexual assaults go unreported in the United States. *The Criminal Justice System: Statistics*, RAINN, https://www.rainn.org/statistics/criminal-justice-system [https://perma.cc/M4C6-WYN9]. Only a small percentage of sexual assault victims undergo sexual assault forensic exams. Linda Carroll, *Police Get Rape Kits in Small Percentage of Cases*, REUTERS (Aug. 7, 2018, 5:43 PM), https://www.reuters.com/article/us-health-sexual-assault/police-get-rape-kits-in-small-percentage-of-cases-idUSKBN1KS2JQ [https://perma.cc/XV7H-47S3].

of routinely searching crime victims' DNA in unrelated criminal investigations had apparently occurred for seven years,[7] and was even regarded by some in the District Attorney's office to be "standard operating procedure in the field,"[8] raising serious questions about how this controversial practice had evaded public scrutiny for so long.

Though its particular facts may be shocking, the San Francisco rape kit case is nothing new. Creative DNA search methods used by police in criminal investigations have grabbed the headlines over the past several years. It was a mere four years prior that police used an open-source recreational genetic genealogy website to triangulate the identity of the Golden State Killer through genetic matches to relatives who had uploaded their genetic data from commercial tests such as 23andMe and Ancestry, inspiring public bewilderment toward this new and surprising approach to forensic investigation.[9] This practice—known as investigative genetic genealogy—recently received renewed attention when anonymous law enforcement sources revealed that Idaho police relied on the same technique to zero in on the suspect in the 2022 University of Idaho homicides, signifying an expansion of this new investigative method beyond cold cases to ones that are still hot.[10]

Commercial genetic databases are not the only surprising alternative sources of genetic data that police have turned to in criminal investigations. A public records lawsuit filed in July 2022 alleges that New Jersey police sought a newborn's blood sample from the New Jersey Department of Health—initially obtained as part of a required public health screening program—to investigate the child's father in connection with a sexual assault from the 1990s.[11] Similarly, in the wake of the San Francisco rape

---

7. *See* Tami Abdollah, *Rape Survivors, Child Victims, Consensual Sex Partners: San Francisco Police Have Used DNA from All of Them for 7 Years*, USA TODAY (Feb. 25, 2022, 1:58 PM), https://www.usatoday.com/story/news/nation/2022/02/23/san-francisco-police-rape-kit-dna-controversy/6854467001/ [https://perma.cc/7GPA-362C].

8. Paybarah, *supra* note 1.

9. *See* Keith Allen, Jason Hanna & Cheri Mossburg, *Police Used Free Genealogy Database to Track Golden State Killer Suspect, Investigator Says*, CNN (Apr. 27, 2018, 2:25 PM), https://www.cnn.com/2018/04/26/us/golden-state-killer-dna-report [https://perma.cc/UZE8-6J99].

10. *See* Heather Tal Murphy, *How Police Actually Cracked the Idaho Killings Case*, SLATE (Jan. 10, 2023, 6:19 PM), https://slate.com/technology/2023/01/bryan-kohberger-university-idaho-murders-forensic-genealogy.html [https://perma.cc/8JG2-3FQ2] ("It was only after investigators utilized a technique reliant on genealogy databases to determine who'd left DNA on a tan leather knife sheath that police requested a search warrant for Kohberger's phone records, according to this source. Up until that point, in late December, he hadn't stood out among all the other [suspects], the source said, something that is reinforced by a close, informed reading of the affidavit.").

11. *See* Verified Complaint, N.J. Off. of the Pub. Def. v. N.J. Dep't of Health, No. MER-L-001210-22 (N.J. Super. Ct. Law Div. July 11, 2022); Emily Mullin, *Police Used a Baby's DNA to Investigate Its Father for a Crime*, WIRED (Aug. 15, 2022, 7:00 AM), https://www.wired.com/story/police-used-a-babys-dna-to-investigate-its-father-for-a-crime/ [https://perma.cc/J8PZ-X88K].

kit case, it was revealed that law enforcement had used California's biobank—which indefinitely stores DNA samples from nearly every baby born in the state—in criminal investigations.[12]

Like questionable DNA database searches, law enforcement DNA collection practices have also garnered significant public attention, especially since the Supreme Court's decision in *Maryland v. King*, which held that police may collect DNA from people who have been arrested for—but not yet convicted of—a crime.[13] Since *King*, police have not only had free reign to collect DNA from arrestees, but they also have enjoyed largely unconstrained latitude to warrantlessly collect DNA from any member of the general public. DNA dragnets, in which police collect and indefinitely store DNA samples from large swaths of the public in order to find a match for DNA recovered from a crime scene, have become increasingly routine.[14] Some prosecutors, most notably the Orange County District Attorney's Office, have built their own DNA databases in a program known colloquially as "Spit and Acquit," where prosecutors offer some defendants charged with petty misdemeanors a dismissal or plea offer in exchange for DNA collection and storage in the prosecutorial database.[15] According to a class action filed in March 2022, New York Police Department detectives have a practice of secretly collecting DNA—including from children—by offering suspects drinks in custodial interrogations to collect their DNA and add the information to a "Suspect Index" for indefinite storage without the individual's knowledge,[16] and even when someone has explicitly refused to

---

12. [B]lood spots [from California's biobank] are being used by law enforcement. We found at least five search warrants and four court orders for identified blood spots before the Golden State Killer case popularized investigative genetic genealogy. Since then, investigators have confirmed newborn blood spots are being used to solve cold cases.

*California Stores DNA from Every Baby: Renewed DNA Privacy Concerns Following SFPD Rape-Kit Allegations*, CBS NEWS SACRAMENTO (Feb. 16, 2022, 9:22 AM), https://www.cbsnews.com/sacramento/news/california-biobank-dna-privacy-concerns/ [https://perma.cc/2QCM-GQWW].

13. Maryland v. King, 569 U.S. 435, 465–66 (2013).

14. *See, e.g.*, Lauren Kirchner, *DNA Dragnet: In Some Cities, Police Go from Stop-and-Frisk to Stop-and-Spit*, PROPUBLICA (Sept. 12, 2016, 8:00 AM), https://www.propublica.org/article/dna-dragnet-in-some-cities-police-go-from-stop-and-frisk-to-stop-and-spit [https://perma.cc/67FZ-8FGK]; Ayyan Zubair, *DNA Dragnets*, SURVEILLANCE TECH. OVERSIGHT PROJECT (Oct. 15, 2019), https://www.stopspying.org/latest-news/2019/10/15/dna-dragnets [https://perma.cc/ZK4S-VQ55].

15. *See* Andrea Roth, *"Spit and Acquit": Prosecutors as Surveillance Entrepreneurs*, 107 CALIF. L. REV. 405, 417 (2019); Jennifer Lynch, Saira Hussain & Andrew Crocker, *EFF Files Amicus Brief Challenging Orange County, CA's Controversial DNA Collection Program*, ELEC. FRONTIER FOUND. (Nov. 10, 2022), https://www.eff.org/deeplinks/2022/11/eff-files-amicus-brief-challenging-orange-county-cas-controversial-dna-collection [https://perma.cc/9KJ4-22SR].

16. *See* Complaint at 5–6, Leslie v. City of New York, No. 1:22-cv-02305, 2022 WL 848169 (S.D.N.Y. Mar. 21, 2022) ("[D]etectives interrogated a 12-year-old boy they suspected of having committed a crime and took his DNA . . . . In the interrogation room, detectives handed him a McDonald's soda. The boy drank the soda and ultimately was escorted out of the room by police. Without the knowledge or consent of the boy or his parents, detectives removed the straw from the soda

consent to providing a DNA sample.[17] Similarly, investigators may rummage through trash to collect DNA from discarded items without a warrant.[18] Increasingly, these DNA collection practices are used in conjunction with search techniques such as the investigative genetic genealogy methods used in the Golden State Killer and University of Idaho homicide cases.[19]

From the pattern of headline-making DNA collection practices and usages in law enforcement investigations emerges the grim reality of "DNA on Demand," where police have frictionless access to vast quantities of genetic information. With DNA collection and storage faster and cheaper than ever—and few legal rules circumscribing genetic data collection and use—law enforcement and private actors have embraced genetic data maximalism, assembling vast, interconnected troves of intimate genetic information that may be searched and used indefinitely, even in ways completely attenuated from the initial DNA collection. What legal rules do exist address particular types of DNA databases or collection tactics only in isolation, and typically only when public attention demands it. One day, the discussion centers around police searches of commercial databases; the next, use of crime victim DNA to investigate victims for later, unrelated crimes, and so on. This approach has proven ineffective. Because of the

---

and had the DNA sample from the straw compared to DNA evidence found at the crime scene. The boy's DNA did not match the crime scene DNA and the charges against him were dropped. However, following the [New York Police Department (NYPD)]'s policy, [the Office of the Chief Medical Examiner] proceeded to store the boy's DNA in its Suspect Index, making him a suspect in future criminal cases involving DNA. His DNA remained in the Suspect Index for more than a year where it was compared against tens of thousands of crime scene samples until his parents were finally able to get it expunged.").

17. *Id.* at 6 ("Even when someone has explicitly refused to consent to providing a DNA sample, NYPD detectives have circumvented that refusal by simply taking the person's DNA without their knowledge. NYPD detectives even circumvent refusals to take the DNA of children. In a February 2020 New York City Council hearing, senior NYPD officials admitted to giving NYPD detectives the discretion to secretly take a child's DNA after the child and their parent have refused to provide it.").

18. *See, e.g.*, Jennifer Lynch, *EFF Challenges Surreptitious Collection of DNA at Iowa Supreme Court*, ELEC. FRONTIER FOUND. (Apr. 9, 2021), https://www.eff.org/deeplinks/2021/04/eff-challenges-surreptitious-collection-dna-iowa-supreme-court [https://perma.cc/R7WJ-WM2U] (describing collection of DNA from a straw that a suspect had used and left behind at a restaurant); Alexia Ramirez, *Police Need a Warrant to Collect DNA We Inevitably Leave Behind*, ACLU (Mar. 10, 2020), https://www.aclu.org/news/privacy-technology/police-need-a-warrant-to-collect-dna-we-inevitably-leave-behind [https://perma.cc/D2X7-CABB].

19. *See* Lynch, *supra* note 18 ("In 2018, the police began working with a company called Parabon Nanolabs, which used the forensic DNA profile to predict the physical appearance of the alleged perpetrator and to generate an image that the Cedar Rapids Police Department released to the public. That image did not produce any new leads, so the police worked with Parabon to upload the DNA profile to a consumer genetic genealogy database called GEDMatch . . . . Through GEDMatch, the police linked the crime scene DNA to three brothers, including the defendant in this case, Jerry Burns. Police then surveilled Mr. Burns until they could collect something containing his DNA. The police found a straw he used and left behind at a restaurant, extracted a profile from DNA left on the straw, matched it to DNA found at the crime scene, and arrested Mr. Burns.").

wide range of collection tactics and databases that police may deploy in investigations, shunting access to one tends merely to divert law enforcement to one of the many others that they may easily access in the absence of substantive legal limits. For example, restrictions on the Combined DNA Index System (CODIS)—the FBI's national DNA database—sparked the expansion of significantly less-regulated state and local databases.[20] Such restrictions also sparked private sector involvement in the forensic genetic surveillance apparatus, with at least some private firms deliberately advertising their services as an end-run around the privacy and quality restrictions of CODIS.[21] Similarly, attempts to regulate state databases are easily sidestepped merely by turning to local databases not subject to the same restrictions.[22] And, while much attention has been given to new state laws that regulate commercial DNA databases,[23] they are likely to suffer from the same fatal flaw.

The law's piecemeal approach—stemming from its treatment of genetic privacy harms as disconnected, rather than as symptoms of single problem—is a familiar theme from other areas of the law that have failed to

20. *See* Jason Kreag, *Going Local: The Fragmentation of Genetic Surveillance*, 95 B.U. L. REV. 1491, 1501 (2015) (describing how "restrictions in the CODIS regulations, which, according to many local law enforcement officials, limit law enforcement's ability to take full advantage of DNA databases to solve crime" led to the fragmentation of DNA databases, allowing state and local agencies to push the boundaries of genetic surveillance and use it in ways not previously permitted under CODIS's comparatively extensive regulatory architecture).

21. *See* ERIN E. MURPHY, INSIDE THE CELL: THE DARK SIDE OF FORENSIC DNA 186–87 (2015) ("The home page for SmallPond, [a private genetic database,] . . . advertises that 'SmallPond may be for you': if you are currently using or considering the use of CODIS for your DNA databasing needs, but are concerned about: the long backlogs at public state and regional DNA labs with CODIS access[,] the profile entry restrictions imposed by CODIS[,] the lack of local criminal elements in the CODIS database[,] the costs and maintenance headaches of the required hardware/network infrastructure[, and] the costs and time of training and certifications required[.]").

22. *See* Jamie Williams, *San Diego Police Target African American Children for Unlawful DNA Collection*, ELEC. FRONTIER FOUND. (Feb. 15, 2017), https://www.eff.org/deeplinks/2017/02/san-diego-police-targets-african-american-children-unlawful-dna-collection [https://perma.cc/GLW2-TE5B] ("[San Diego Police Department's (SPDP's)] policy seems to intentionally sidestep the minimal protections the California legislature built into California's DNA collection law, Cal. Penal Code § 296. . . . SDPD's policy acknowledges the limits in Section 296, but it gets around these limits by keeping the DNA profiles collected via its 'consent' searches in a local database, rather than adding them into the statewide DNA database. As the policy points out, Section 296 only governs DNA seized for inclusion in the statewide database. So, as the Voice of San Diego puts it, 'the San Diego Police Department has found a way around state law.'").

23. *See, e.g.*, Jennifer Lynch, *Maryland and Montana Pass the Nation's First Laws Restricting Law Enforcement Access to Genetic Genealogy Databases*, ELEC. FRONTIER FOUND. (June 7, 2021), https://www.eff.org/deeplinks/2021/06/maryland-and-montana-pass-nations-first-laws-restricting-law-enforcement-access [https://perma.cc/2NDG-ERY8]; Laura Geary, Online Note, *A Critical Eye Toward Commercial DNA Database Criminal Procedures*, U. CHI. L. REV. ONLINE (July 8, 2022), https://lawreviewblog.uchicago.edu/2022/07/08/geary-dna-databases/ [https://perma.cc/QM4M-NAJJ] (discussing Maryland's and Montana's 2021 laws regulating forensic genetic genealogical DNA searches).

safeguard privacy interests.[24] So too are the social attitudes surrounding the use of DNA analysis in criminal investigations. Some argue that genetic data merits little or no protection in the criminal investigation context because of society's strong interest in deterring crime,[25] and others echo the famous rejoinder to any argument for privacy, if you have "nothing to hide[, you] have nothing to fear."[26] These pervasive ideas are far from fatal to a conception of genetic privacy. Rather, they underscore the urgent need for a comprehensive picture of the myriad ways that genetic information is collected, stored, and used in criminal investigations, and the harms wrought by invasions of genetic privacy. Only by appraising the severe privacy harms suffered across the wide variety of DNA collection methods and databases can we begin to view the many variations of genetic privacy violations as a single problem, which is crucial in order to meaningfully safeguard privacy interests.

This Note seeks to do that. Part I provides an overview of the different types of DNA databases and collection techniques that police may employ in criminal investigations. Part II assesses harms to civil rights and liberties wrought by invasions of genetic privacy in criminal investigations, irrespective of particular DNA collection method or database type. Part III identifies the objective of regulation—to safeguard against genetic privacy violations across contexts—and proposes guiding principles for legislatures to consider to this end. Part IV anticipates and addresses a series of objections to this proposal.

---

24. *See, e.g.*, DANIELLE KEATS CITRON, THE FIGHT FOR PRIVACY xvii (2022) (describing the law's failure to safeguard intimate privacy) ("Privacy violations are treated as disconnected problems or normal market practices, rather than as endemic societal challenges."); Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. REV. 793, 816 (2022) (constructing a typology for courts to understand privacy harms) ("A major complicating dimension of many privacy harms is that they are small but numerous. . . . Privacy harms often involve the aggregation of many small harms to each individual, which is compounded by the aggregation of all these harms to many individuals."); Woodrow Hartzog & Evan Selinger, *Surveillance as Loss of Obscurity*, 72 WASH. & LEE L. REV. 1343, 1370 (2015) ("[A] patchwork approach to resolving cases has resulted in 'doctrinal gaps,' rather than a unified paradigm of surveillance theory . . . .").

25. *See, e.g.*, Kirchner, *supra* note 14. In a conversation with a Pennsylvania Director of Public Safety, the director observed that state and local DNA databases built with the assistance of private firms have "probably been the greatest innovation in local law enforcement since the bulletproof vest. . . . It stops crime in its tracks. . . . So why everyone's not doing it, I don't know." *Id.*

26. *See, e.g.*, Dan Rodricks, *DNA: Why Wait for an Arrest?*, BALT. SUN (May 2, 2012), https://web.archive.org/web/20210622002519/https://www.baltimoresun.com/opinion/bs-xpm-2012-05-02-bs-ed-rodricks-dna-20120502-story.html [https://perma.cc/9UNA-JUNY].

## I. UNDERSTANDING DNA DATABASES AND COLLECTION PRACTICES

This Part canvasses the range of DNA databases used by police in the course of criminal investigations. Section A describes CODIS,[27] the DNA database with the most rigorous regulatory framework. Then, Sections B, C, and D explore the comparatively unregulated non-CODIS databases to set the groundwork for how CODIS's extensive regulatory structure is rendered essentially meaningless by alternative databases not subject to the same regulations.

### *A. CODIS*

Congress created CODIS in 1994, and designated the FBI as its regulator.[28] "[W]hen the initial version of the CODIS software was being developed, the FBI Laboratory convened a group of privacy advocates to obtain feedback on its plans for this new law enforcement tool."[29] From this came the extensive regulatory scheme for CODIS promulgated by Congress and the FBI, which governs whose DNA may be uploaded to the database, the types of records stored and searched, and the procedures for storing, accessing, and retaining genetic data.[30] The following Subsections detail those procedural requirements and law enforcement perceptions of these requirements as too stringent, which has laid the groundwork for the construction and use of alternative, less regulated DNA databases in criminal investigations.

#### *1. CODIS Procedural Requirements*

The first procedural requirement concerns laboratory participation in CODIS. In order to participate in CODIS, laboratories must be

27. A note on terminology: Combined DNA Index System (CODIS) is "the generic term used to describe the FBI's program of support for criminal justice databases . . . . The National DNA Index System or NDIS is considered one part of CODIS, the national level, containing the DNA profiles contributed by federal, state, and local participating forensic laboratories." *Frequently Asked Question on CODIS and NDIS*, FBI, https://www.fbi.gov/how-we-can-help-you/dna-fingerprint-act-of-2005-expungement-policy/codis-and-ndis-fact-sheet [https://perma.cc/BT3E-N2HD]. In this Note, the term CODIS is used to refer generally to the FBI's national DNA database. In the limited instances where NDIS is instead used, it refers to the same.

28. *See* DNA Identification Act of 1994, 42 U.S.C. § 14132 (transferred to 34 U.S.C. § 12592).

29. FBI LAB'Y, NATIONAL DNA INDEX SYSTEM (NDIS) OPERATIONAL PROCEDURES MANUAL 5 (2016), https://ucr.fbi.gov/lab/biometric-analysis/codis/ndis-procedures-manual [https://perma.cc/958L-WLFC].

30. *See generally id.* (outlining CODIS procedural requirements).

professionally accredited and employ qualified DNA analysts,[31] undergo annual audits, [32] and comply with federal expungement rules.[33]

The second procedural requirement concerns types of genetic profiles which may be included in CODIS. First, DNA samples that are "voluntarily submitted solely for elimination purposes" may not be included in CODIS.[34] For example, a crime victim's genetic profile that was collected only to distinguish the victim's genetic information from that of a criminal suspect may not be included in CODIS. Second, a DNA record submitted solely for investigative purposes is prohibited from inclusion in CODIS,[35] and only DNA identification records from convicted individuals and arrestees may be included in CODIS.[36] Third, no personally identifiable information about individuals who provided DNA samples is maintained in the DNA identification records stored in CODIS.[37] Instead, DNA records in CODIS contain a Specimen Identification Number and Agency Identifier.[38] Only once a match has been confirmed may personally identifying information be released.[39]

The third procedural requirement concerns searches. Generally, a routine search of CODIS is run twice a week to "search new and modified DNA records against all records" in the database.[40] There are limited exceptions which allow for the comparison of a target DNA record against DNA records contained in CODIS without resulting in the target record being included or uploaded into the national database.[41] In all other cases, laboratories use the routine upload and semiweekly search procedure for searching CODIS DNA records. If a search yields a match, "a candidate match list will then be reviewed, evaluated, and information released in accordance with [CODIS disclosure requirements]."[42]

The fourth procedural requirement concerns disclosures. Because no personally identifiable information about individuals who provided DNA

31. *Id.* at 12–13.

32. *Id.* at 8. The DNA Identification Act requires that laboratories participating in CODIS "undergo external audits, not less than once every 2 years, that demonstrate compliance with standards established by the Director of the Federal Bureau of Investigation." 42 U.S.C. § 14132(b)(2)(B) (transferred to 34 U.S.C. § 12592(b)(2)(A)(ii)).

33. *Id.* § 14132(d) (transferred to 34 U.S.C. § 12592(d)).

34. *Id.* § 14132(a)(1)(C) (transferred to 34 U.S.C. § 12592(a)(1)(C)).

35. *See* Privacy Act of 1974; New System of Records, 61 Fed. Reg. 37495, 37498 (July 18, 1996).

36. 42 U.S.C. § 14132(a)(1)–(4) (transferred to 34 U.S.C. § 12592(a)(1)–(4)).

37. *See* Privacy Act of 1974; New System of Records, 61 Fed. Reg. at 37497–98. As it is used here, "personally identifiable information" excludes the genetic profile itself.

38. FBI LAB'Y, *supra* note 29, at 67.

39. *See id.* at 50.

40. *Id.* at 48.

41. *See id.* at 48–49.

42. *Id.*

samples is maintained in CODIS, names and personally identifiable information cannot be disclosed directly from CODIS.[43] However, the DNA records of one criminal justice agency may be disclosed to another criminal justice agency when there is a potential DNA match.[44]

Finally, regulations require the expungement—or deletion—of profiles from CODIS in two scenarios. First, genetic profiles of convicted offenders must be deleted if their conviction has been overturned.[45] Second, genetic profiles of arrestees must be deleted if they were acquitted, their charges were dismissed, or "no charges were filed within the applicable time period."[46]

### *2. Perceived Limitations*

The regulations that govern CODIS are quite stringent, which has led many investigators to believe that it does not adequately meet their needs. Early adopters of local DNA databases have argued that the CODIS regulations on genetic profile inclusion and search are too restrictive, and that because CODIS mostly comprises genetic profiles from "known violent offenders who are often serving lengthy prison sentences," it is an "ineffective crime-solving tool."[47] These perceived limitations—combined with advances in DNA processing,[48] federal forfeiture laws,[49] and corporate interests[50]—have incentivized law enforcement to build out state and local DNA databases or turn to alternative sources of securing genetic data, such as commercial and public health databases.[51]

---

43. *See* Privacy Act of 1974; New System of Records, 61 Fed. Reg. 37495, 37497 (July 18, 1996).

44. *See id.* at 37498, 37496.

45. FBI LAB'Y, *supra* note 29, at 33.

46. *Id.* at 33; DNA Identification Act of 1994, 42 U.S.C. § 14132(d) (transferred to 34 U.S.C. § 12592(d)).

47. *See* Kreag, *supra* note 20, at 1501–02 (describing law enforcement officers' frustrations over CODIS regulations and their perceived limitations).

48. Advances in DNA processing mean that police no longer need to rely on laboratories to perform DNA analysis, can process DNA more cheaply than before, and can analyze very small amounts of genetic material which allows them to investigate non-violent crimes such as property crimes. *Id.* at 1504–05.

49. Counterintuitively, some state and local DNA databases are funded through federal—not local—funds by way of federal forfeiture laws, which "return money to local law enforcement officials in exchange for their participation in federal task forces," meaning that local agencies have largely been able to "bypass the local budget process and the limitations it imposes on other law enforcement surveillance techniques." *Id.* at 1505–06.

50. The privatization of DNA processing has also facilitated local database expansion, as private firms serve as gap-fillers in jurisdictions that, for example, do not have their own laboratory. *Id.* at 1501–07.

51. *Id.*

### *B. State and Local Databases*

The expansion of and increased reliance on state and local DNA databases is a well-documented phenomenon.[52] Crucially, state and local databases are not subject to the same extensive regulations as CODIS.[53] States and localities are largely free to determine their own rules regarding which types of samples may be added to the database and how they may be searched and stored.[54] For example, many state and local databases allow for the inclusion of genetic profiles of victims, collected only to distinguish their genetic profile from that of the perpetrator,[55] as seen in the San Francisco rape kit case.[56] Such practices stand in stark contrast to CODIS's comparatively more protective regulations, which only allow for the inclusion of DNA from arrestees and convicted persons.[57]

In the absence of regulations governing the types of genetic profiles that may be included, state and local databases also frequently rely on DNA collected pursuant to methods that push the envelope of lawful investigative tactics.[58] Because of their extensive reliance on obtaining DNA samples through so-called "consent searches" or through surreptitious collection of "abandoned" DNA, the resulting databases "operate largely beyond reach of the Fourth Amendment."[59] An overview of consent-based DNA collection practices and abandoned DNA collection practices frequently employed by police is detailed in the Subsections below.

#### *1. "Consent"-Based DNA Collection Practices*

It is a well-settled principle that searches conducted pursuant to the consent of the individual being searched are valid exceptions to the Fourth

52. *See, e.g.*, *id.*; Stephen Mercer & Jessica Gabel, *Shadow Dwellers: The Underregulated World of State and Local DNA Databases*, 69 N.Y.U. ANN. SURV. AM. L. 639, 667–80 (2014); MURPHY, *supra* note 21, at 180–83 (describing how Maryland's state-run DNA database allowed police to arrest a man who submitted DNA for exclusion purposes for an unrelated commercial burglary committed four years prior); Roth, *supra* note 15, at 407–33 (documenting the Orange County District Attorney's Office's maintenance of a prosecutorial DNA database and practice of collecting DNA as part of misdemeanor dismissals or plea offers).

53. *See* Kreag, *supra* note 20, at 1503.

54. *See id.*

55. "[L]ocal databases also often include genetic profiles of suspects (including juvenile suspects), witnesses, crime victims, family members of victims, and citizens who responded to police DNA dragnets, which sometimes follow violent, unsolved crimes." *Id.* at 1497.

56. *See* Abdollah, *supra* note 7.

57. *See supra* Section I.A.1.

58. *See* MURPHY, *supra* note 21, at 168–69.

59. *See* Kreag, *supra* note 20, at 1498–99. Consent searches and abandonment of property are two judicially recognized exceptions to the Fourth Amendment warrant requirement. *See infra* Sections II.A.1, I.B.2.

Amendment warrant requirement.[60] Whether a search is consensual depends only on whether consent was freely and voluntarily given "rather than the product of duress or coercion."[61] Beyond the baseline requirement that consent must be voluntary in order to be valid, there are no restrictions on consent searches. As a result, the practice of DNA collection pursuant to an individual's alleged consent has received great deference, enabling campaigns of warrantless DNA collection such as DNA dragnets and prosecutorial Spit and Acquit programs.

*a. DNA Dragnets*

A DNA dragnet is a practice in which police collect "DNA samples from large swaths of the public in order to find a match with DNA recovered at crime scenes."[62] DNA dragnets may consist of police knocking on doors of residences or businesses within the vicinity of a crime,[63] stopping individuals on the street,[64] or asking individuals to consent to DNA collection during a traffic stop.[65] Because DNA dragnets are premised on consent, the propriety of this DNA collection method has largely evaded scrutiny.

*b. Prosecutorial Spit and Acquit Programs*

Prosecutorial Spit and Acquit programs—where prosecutors offer some defendants charged with petty misdemeanors a dismissal or plea offer in exchange for DNA collection and inclusion in the prosecutorial database—also rely on consent as a justification.[66] As of 2019, over 150,000 people had agreed to the Orange County District Attorney's Spit and Acquit program since its inception in 2007, making it the "largest 'consent'-based law enforcement DNA database in the country."[67] "[N]early every

60. *See* Ohio v. Robinette, 519 U.S. 33, 39–40 (1996).

61. Schneckloth v. Bustamonte, 412 U.S. 218, 227 (1973).

62. Zubair, *supra* note 14.

63. Andrew Whalen, *NYPD's 'Knock-and-Spit' DNA Database Makes You a Permanent Suspect*, NEWSWEEK (Feb. 11, 2019, 12:29 PM), https://www.newsweek.com/police-dna-database-nypd-swab-testing-collection-new-york-1326722 [https://perma.cc/W46T-4JFG].

64. *See, e.g.*, Williams, *supra* note 22.

65. *See, e.g.*, Kirchner, *supra* note 14 ("[T]o compile samples for comparison, some jurisdictions also have quietly begun asking people to turn over DNA voluntarily during traffic stops, or even during what amount to chance encounters with police. In Melbourne, [Florida,] riding a bike at night without two functioning lights can lead to DNA swab—even if the rider is a minor.").

66. *See* Roth, *supra* note 15, at 408.

67. *Id.* at 405, 408, 417. This figure perhaps comes as no surprise given the exceptionally high rates of criminal convictions obtained through plea bargaining. Emily Yoffe, *Innocence Is Irrelevant*, ATLANTIC (Sept. 2017), https://www.theatlantic.com/magazine/archive/2017/09/innocence-is-irrelevant/534171/ [https://perma.cc/YY3G-AFWE].

misdemeanor plea deal in Orange County is now conditioned on providing DNA."[68]

### *2. Surreptitious "Abandoned" DNA Collection*

Like consent, abandonment is another constitutional doctrine that allows police to collect an individual's DNA without first securing a warrant. The abandonment doctrine stipulates that a Fourth Amendment search or seizure does not occur when police inspect or collect abandoned property, and therefore no warrant is necessary.[69] Courts "tend[] to approach abandonment in terms of the view that the Fourth Amendment protects individuals against official intrusion into areas where they have a 'reasonable expectation of privacy.'"[70] The abandonment doctrine has largely been extended to apply to the collection of DNA that has been left on surfaces that individuals have touched.[71] Therefore, police may collect DNA from surfaces touched by an individual in an interrogation room or from discarded objects obtained by rummaging through an individual's trash. Collection of "abandoned" DNA is typically done surreptitiously, without an individual's consent, and is sometimes performed even when an individual has explicitly refused to consent to DNA collection.[72]

While conventionally speaking, neither "consent"-based searches nor surreptitious collection of "abandoned" DNA run afoul of the Fourth Amendment, the appropriateness of applying these doctrines to genetic information has rightfully been called into question.[73] The harms wrought by these two DNA collection methods are detailed in Section II.A below.

## *C. Commercial Databases*

The use of commercial DNA databases in criminal investigations—a practice known as investigative genetic genealogy—garnered public

---

68. Roth, *supra* note 15, at 408.

69. *See* Hester v. United States, 265 U.S. 57, 58 (1924).

70. John P. Ludington, *Search and Seizure: What Constitutes Abandonment of Personal Property Within Rule that Search and Seizure of Abandoned Property Is Not Unreasonable—Modern Cases*, 40 A.L.R.4th 381 (1985).

71. *See* Elizabeth E. Joh, *Reclaiming "Abandoned" DNA: The Fourth Amendment and Genetic Privacy*, 100 NW. U. L. REV. 857, 858–59 (2006).

72. *See, e.g.*, Complaint at 5–6, Leslie v. City of New York, No. 1:22-cv-02305, 2022 WL 848169 (S.D.N.Y. Mar. 21, 2022); Raynor v. State, 99 A.3d 753, 756, 768 (Md. 2014) (holding that police did not conduct a search by testing genetic material that suspect left on chair during interview at police station even after suspect declined to consent to DNA collection), *cert. denied*, 574 U.S. 1192 (2015).

73. *See, e.g.*, Zubair, *supra* note 14; Roth, *supra* note 15, at 440–47; Holly K. Fernandez, *Genetic Privacy, Abandonment, and DNA Dragnets: Is Fourth Amendment Jurisprudence Adequate?*, HASTINGS CTR. REP., Jan.–Feb. 2005, at 21, 22–23; Joh, *supra* note 71, at 862–73.

attention when the technique was used to solve the then-cold Golden State Killer case.[74] In that case, investigators first uploaded the suspect's DNA profile to GEDMatch,[75] an open-source database where people upload their raw genetic data from popular commercial genetic testing kits such as 23andMe and Ancestry.[76] Using partial genetic matches to relatives, investigators then constructed a family tree and triangulated the identity of the serial murderer.[77]

Two factors enabled police to conduct this search: the third-party doctrine and GEDMatch's terms of service. The third-party doctrine is a legal principle often invoked in support of allowing law enforcement to search property or information voluntarily provided to a third party without first needing to obtain a warrant.[78] However, the Supreme Court has recognized some limits on the third-party doctrine, most notably in *Carpenter v. United States*, in which the Court held that a warrant is required to search the record a cell phone creates of its user's movements, even though the user's location information was shared with a third party.[79] The

74. *See* Allen et al., *supra* note 9; *see also* Heather Murphy, *She Helped Crack the Golden State Killer Case. Here's What She's Going to Do Next.*, N.Y. TIMES (Aug. 29, 2018), https://www.nytimes.com/2018/08/29/science/barbara-rae-venter-gsk.html [https://perma.cc/NT8B-RZES] (describing how the investigative genetic genealogist who helped identify the Golden State Killer "has inspired others to help law enforcement with unsolved cases, as well as an ethics and privacy debate").

75. Murphy, *supra* note 74.

76. *About GEDMatch: Genealogy Research Reimagined and Expanded*, GEDMATCH, https://www.gedmatch.com/about/ [https://perma.cc/GGD2-GCLT]. The market-leaders in the direct-to-consumer genetic testing sector, 23andMe and Ancestry, do not easily enable law enforcement searches on their platforms. *See 23andMe Guide for Law Enforcement*, 23ANDME, https://www.23andme.com/law-enforcement-guide [https://perma.cc/33YX-2TDT] ("23andMe chooses to use all practical legal and administrative resources to resist requests from law enforcement, and we do not share customer data with any public databases, or with entities that may increase the risk of law enforcement access."); *Ancestry Guide for Law Enforcement*, ANCESTRY, https://www.ancestry.com/c/legal/lawenforcement [https://perma.cc/4VSV-D987] ("Ancestry does not voluntarily cooperate with law enforcement. . . . [W]e require all government agencies seeking access to Ancestry customers' data to follow valid legal process and **do not** allow law enforcement to use Ancestry's services to investigate crimes or to identify human remains."). However, if individuals upload raw genetic data from 23andMe or Ancestry to GEDMatch, the Terms of Service of GEDMatch then apply.

77. Dan Barry, Tim Arango & Richard A. Oppel Jr., *The Golden State Killer Left a Trail of Horror with Taunts and Guile*, N.Y. TIMES (Apr. 28, 2018), https://www.nytimes.com/2018/04/28/us/golden-state-killer-joseph-deangelo.html [https://perma.cc/Z3T4-ZKSW].

78. *See, e.g.*, United States v. Miller, 425 U.S. 435, 440 (1976) (finding no expectation of privacy in financial records held by a bank); Smith v. Maryland, 442 U.S. 735, 745 (1979) (finding no expectation of privacy in records of dialed telephone numbers conveyed to telephone company).

79. 138 S. Ct. 2206, 2219 (2018) (recognizing a legitimate expectation of privacy in the whole of an individual's movements as captured through cell-site information location (CSLI)). According to the *Carpenter* Court, "the nature of the particular [information] sought" must be considered "to determine whether 'there is a legitimate expectation of privacy concerning their contents.'" *Id.* (quoting *Miller*, 425 U.S. at 442). The *Carpenter* Court insisted that its holding was "narrow," and explicitly declined to call into question even related technologies such as "real-time CSLI or 'tower dumps' (a download of information on all the devices that connected to a particular cell cite during a particular interval)" or "conventional surveillance techniques and tools." *Id.* at 2220. However, many legal

propriety of applying the third-party doctrine in the context of law enforcement use of consumer genetic databases to identify suspects through relatives who have used the service is an open question that many other scholars have grappled with.[80]

Terms of service also influence the propriety of database searches by law enforcement. At the time when police used GEDMatch in the Golden State Killer investigation, users had "no choice, and often little awareness," as to whether police could access and use their genetic profiles in criminal investigations.[81] This policy has since changed, and users must now explicitly opt in to allow law enforcement to access their profiles.[82] However, because investigative genetic genealogy often involves triangulating suspects' identities through genetic data uploaded by relatives, individuals who have not opted in to law enforcement access may nevertheless be identified if a distant relative has opted in.[83] Additionally, police agencies have been able to obtain warrants to compel GEDMatch to open up its full database for investigation, including the profiles of individuals who have not opted in to law enforcement access.[84] Exactly how such a warrant must be worded to be valid remains an open question.[85]

---

arguments about searches of personal data have seized upon *Carpenter*'s loosening of the third-party doctrine, including in the context of law enforcement searches of commercial genetic databases. *See, e.g.*, Natalie Ram, *Genetic Privacy After* Carpenter, 105 VA. L. REV. 1357, 1358 (2019) (applying *Carpenter*'s test to argue that "genetic information is precisely the sort of data in which individuals may ordinarily maintain an expectation of privacy, even when that data is in third-party hands").

80. *See, e.g.*, Ram, *supra* note 79, at 1375–81; Paul Ohm, *The Many Revolutions of* Carpenter, 32 HARV. J.L. & TECH. 357, 383–85 (2019) (concluding that the propriety of warrantless searches of "[d]atabases of [m]edical [r]ecords and [g]enetic [i]nformation" is "[u]ncertain" under *Carpenter*'s test).

81. *See* Natalie Ram, *The Genealogy Site that Helped Catch the Golden State Killer Is Grappling with Privacy*, SLATE (May 29, 2019, 7:30 AM), https://slate.com/technology/2019/05/gedmatch-dna-privacy-update-law-enforcement-genetic-geneology-searches.html [https://perma.cc/X8QD-ZQYR].

82. *Id.* As of August 2020, nearly two-thirds of GEDMatch's users opted out of law enforcement access. Heather Murphy, *Why a Data Breach at a Genealogy Site Has Privacy Experts Worried*, N.Y. TIMES (Aug. 1, 2020), https://www.nytimes.com/2020/08/01/technology/gedmatch-breach-privacy.html [https://perma.cc/WYY8-GKHZ].

83. *See* Ram, *supra* note 81.

84. Kashmir Hill & Heather Murphy, *Your DNA Profile Is Private? A Florida Judge Just Said Otherwise*, N.Y. TIMES (Dec. 30, 2019), https://www.nytimes.com/2019/11/05/business/dna-database-search-warrant.html [https://perma.cc/FP9K-NXS3] (discussing a case in which a Florida state judge issued a warrant for a search of the entire GEDMatch database).

85. *See* Jocelyn Kaiser, *A Judge Said Police Can Search the DNA of 1 Million Americans Without Their Consent. What's Next?*, SCIENCE (Nov. 7, 2019), https://www.science.org/content/article/judge-said-police-can-search-dna-millions-americans-without-their-consent-what-s-next [https://perma.cc/6YZL-C467] ("If one of these companies declines to comply with the warrant and challenges the basis of it, that may be the most direct route for evaluating whether and how these warrants can and must be worded in order to be valid.").

### *D. Public Health Biobanks*

Every state collects and analyzes blood samples from newborns as part of public health screening programs that test for a wide variety of disorders, typically without seeking affirmative parental consent.[86] Police have recently tapped these public health databases in criminal investigations.[87] "[M]ore than a quarter of U.S. states have no discernible policy in place regarding law enforcement access, while nearly a third may permit access in some circumstances."[88] "For some states . . . regulatory provisions do not require a warrant to compel disclosure."[89] As other scholars have argued, these searches likely run afoul of the Fourth Amendment's protection against unreasonable searches and seizures.[90]

## II. GENETIC PRIVACY HARMS

Invasions of genetic privacy carry significant individual and collective harms. Like other types of privacy harms, genetic privacy harms present several challenges that make their legal recognition difficult.[91] Typical legal conceptions of harm tend to have only an "individualistic focus and heavily favor tangible physical and financial injuries that occur immediately."[92] Privacy harms, on the other hand, may be minor from the standpoint of each individual but substantial "from the standpoint of society, where the harm to everyone is aggregated."[93] "Privacy harms often involve increased risk of future harm," which individuals and the law alike famously struggle to conceptualize and appreciate.[94] Finally, privacy harms involve a significant relational dimension, as an intrusion on one person's privacy may facilitate the intrusion of another person's privacy.[95]

This Part canvasses the landscape of genetic privacy violations wrought by DNA on Demand, ultimately seeking to render legible the harms to

86. *See* Natalie Ram, *America's Hidden National DNA Database*, 100 TEX. L. REV. 1253, 1254, 1261 (2022).

87. *See* Mullin, *supra* note 11 (New Jersey police seeking DNA from newborn public health screening database); *California Stores DNA from Every Baby*, *supra* note 12 (California police seeking the same).

88. Ram, *supra* note 81, at 1258.

89. *Id.* at 1323.

90. *Id.* at 1312–23 (arguing that warrantless law enforcement use of newborn screening databases violates the Fourth Amendment and is not immunized by doctrinal exceptions to the warrant requirement such as the special needs doctrine and the third-party doctrine).

91. *See* Citron & Solove, *supra* note 24, at 816 n.143 (citing Ignacio N. Cofone & Adriana Z. Robertson, *Privacy Harms*, 69 HASTINGS L.J. 1039, 1041 (2018) ("[P]rivacy harms are hard to pin down.")).

92. *Id.* at 797.

93. *Id.* at 816.

94. *Id.*

95. *See id.* at 859–61.

individual and collective privacy that flow from the overcollection and overuse of genetic data in criminal investigations. By focusing more on the privacy *harms* wrought by DNA overcollection and overuse—and less on particular collection methods, types of DNA databases, or types of database searches—the law can overcome its myopic procedural focus and move toward sensible substantive limits on law enforcement access to and use of genetic information. Without an appreciation of the full breadth of harm wrought by DNA overcollection and overuse, laws will be fatally underinclusive, and tend only to divert law enforcement to one of the many other collection methods or databases at their disposal. Appraising genetic privacy harms—and centering the regulatory discussion around preventing these harms—is therefore crucial to curb the most negative societal impacts and intrusions on civil liberties that flow from the DNA on Demand regime.

Significantly, genetic privacy harms are not distributed or felt equally across society. Because law enforcement has been given wide latitude to decide who to target for sample collection and inclusion, "police [often] seek[] out the 'usual suspects'—poor people of color—to secure DNA samples for these databases,"[96] thus subjecting them to a higher degree of surveillance. Because this disparate impact is frequently experienced concurrently with other privacy harms, discussion of racial disparities is incorporated where relevant in the Sections below.

### *A. Harms from Overcollection*

With few regulations circumscribing collection of DNA by law enforcement and a judicial *carte blanche* to collect DNA through dragnets, Spit and Acquit programs, and surreptitious collection, law enforcement has barreled forward in embracing a "more is more" approach to DNA collection.[97] The law's patchwork approach to genetic privacy has failed to appreciate the individual and collective privacy harms wrought by this ethos of genetic data maximalism. This Section explores those harms that flow from DNA overcollection by law enforcement.

#### *1. Coerced Consent, Unwitting Consent, and Inconsentability*

Consent is the legal basis for DNA collection practices such as DNA dragnets and prosecutorial Spit and Acquit programs.[98] There is a strategic reason for this: consent is a judicially recognized exception to the Fourth

96. Kreag, *supra* note 20, at 1497.
97. *See* MURPHY, *supra* note 21, at 304.
98. *See supra* Sections I.B.1.a, b.

Amendment warrant requirement.[99] Whether a search was consensual depends only on whether consent was freely and voluntarily given.[100] Even if an individual is not aware of his or her right to refuse to consent to the search, consent is legally enforceable.[101] There are three major issues with collecting DNA pursuant to an individual's consent. The first is the risk of coerced consent, which occurs when an individual feels pressured into consenting to DNA collection.[102] The second issue is unwitting consent, which occurs when individuals do not understand the scope or the consequences of what they are consenting to.[103] The final issue is inconsentability, which is the notion that even if valid individual consent can be given for DNA collection, permission for such surveillance impermissibly conflicts with collective privacy interests and therefore should not be enforceable.[104]

Consent searches have been widely criticized as being easily susceptible to coercion. As Justice Marshall explained in his *Schneckloth* dissent, "all the police must do is conduct what will inevitably be a charade of asking for consent. If they display any firmness at all, a verbal expression of assent will undoubtedly be forthcoming."[105] Justice Marshall's prediction is borne out in the data, where, for example, an overwhelming majority of individuals consent to searches during traffic stops when requested.[106] Evaluations of the voluntariness of consent are themselves susceptible to bias, and "consistently underestimate the pressure to comply with intrusive requests."[107] "People may worry that refusing to provide the [DNA] sample

99. Schneckloth v. Bustamonte, 412 U.S. 218, 222 (1973) (discussing that consent alone is a legal basis for a search).

100. *See* Bumper v. North Carolina, 391 U.S. 543, 548 (1968); *see also* United States v. Mendenhall, 446 U.S. 544, 557 (1980).

101. *Schneckloth*, 412 U.S. at 245 n.33.

102. *See, e.g.*, Lynch et al., *supra* note 15 (discussing the risk of coerced consent in the context of the Orange County District Attorney's Office Spit and Acquit program).

103. The phrase "unwitting consent" is borrowed from Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 WASH. U. L. REV 1461, 1478 (2019). Richards and Hartzog note that unwitting consent "can take at least three forms, including not understanding the legal agreement, not understanding the technology being agreed to, or not understanding the practical consequences or risks of agreement." *Id.* at 1466.

104. *See generally* Evan Selinger & Woodrow Hartzog, *The Inconsentability of Facial Surveillance*, 66 LOY. L. REV. 33 (2020) (discussing the inconsentability of biometric surveillance technologies).

105. 412 U.S. at 284 (Marshall, J., dissenting).

106. *See* Adam Schwartz, *So-Called "Consent Searches" Harm Our Digital Rights*, ELEC. FRONTIER FOUND. (Jan. 14, 2021), https://www.eff.org/deeplinks/2021/01/so-called-consent-searches-harm-our-digital-rights [https://perma.cc/78MG-L7HK] ("[S]tatistics on all traffic stops in Illinois, for 2015, 2016, 2017, and 2018, show that about 85% of white drivers and about 88% of minority drivers grant consent.").

107. Roseanna Sommers & Vanessa K. Bohns, *The Voluntariness of Voluntary Consent: Consent Searches and the Psychology of Compliance*, 128 YALE L.J. 1962, 1962 (2019) ("This is problematic because it indicates that a key justification for suspicionless consent searches—that they are voluntary—relies on an assessment that is subject to bias.").

will raise suspicions that they were involved in the crime," or may "feel it is their duty to help [with the investigation,] even if they think the request is unconstitutional."[108] Alternatively, people may simply not be aware of their right to refuse, although recent scholarship suggests that requiring police to advise citizens of their right to refuse consent may have little effect, because "[t]he social demands of police-citizen interactions persist even when people are informed of their rights."[109] In high-pressure situations, such as bargaining with a prosecutor for a misdemeanor dismissal or being stopped on the street by police, consent is largely a "legal fiction."[110]

Importantly, relying on consent to justify DNA collection amplifies racial inequities. "[W]hen decisionmakers have a high degree of subjective discretion, . . . [t]here is a greater risk of racial and other bias."[111] With no degree of suspicion required to ask an individual to consent to a search, the risk of racial bias is extremely high.[112] Some critics of DNA dragnets have drawn a comparison to controversial stop-and-frisk policies, which disproportionately target individuals—and in some cases entire communities—of color.[113] For example, in New York, over 360 Black men were swept up in a "race-biased dragnet" as part of a murder investigation.[114] Racial minorities are more likely to be asked to consent to a search, and rates of compliance are high among all groups.[115] The disparate impact flowing from consent searches on communities of color must be weighed heavily when considering regulatory solutions.

Even if consent is uncoerced, there is the risk that it is unwitting, meaning that individuals do not understand the scope of what they are consenting to, or the consequences of providing a DNA sample. Mere procedural requirements such as having individuals sign a consent form—as the Orange County District Attorney's Office does in its Spit and Acquit

108. Fernandez, *supra* note 73, at 22.

109. Sommers & Bohns, *supra* note 107, at 1962.

110. *See* Lynch et al., *supra* note 15.

111. *See* Schwartz, *supra* note 106.

112. *See id.*

113. "It's genetic stop-and-frisk . . . . It is just like what we saw in stop-and-frisk where police are targeting vulnerable communities, they are targeting Black and LatinX communities and they are collecting DNA from those communities." Dean Meminger, *Exclusive: NYPD DNA Database Continues to Grow, Legal Aid Society Says*, SPECTRUM NEWS NY1 (July 2, 2020, 11:02 PM), https://www.ny1.com/nyc/all-boroughs/news/2020/07/02/nypd-dna-database-continues-to-grow-legal-aid-society-says [https://perma.cc/QG26-ZTS6].

114. Jan Ransom & Ashley Southall, *'Race-Biased Dragnet': DNA from 360 Black Men Was Collected to Solve Vetrano Murder, Defense Lawyers Say*, N.Y. TIMES (Mar. 31, 2019), https://www.nytimes.com/2019/03/31/nyregion/karina-vetrano-trial.html [https://perma.cc/Y84Q-3TAP] ("[A] person with knowledge of the investigation, who spoke on the condition of anonymity, said it was true investigators initially thought the assailants might be white and that the police later had sought saliva samples from hundreds of [B]lack men in the search for the killer.").

115. Sommers & Bohns, *supra* note 107, at 2009.

program—do not meaningfully safeguard genetic privacy interests.[116] First, individuals may not read or understand consent forms.[117] Second, consent forms do not adequately convey the stakes of providing a DNA sample. As Andrea Roth writes of one Spit and Acquit participant:

> [I]n explaining why she was not concerned about giving a sample, [the participant] said, "I'm not a murderer," meaning she saw no issue with giving up her DNA if she does not plan to commit a DNA-solvable offense. But . . . innocent people might also wish to avoid database inclusion. To name a few, concerns include potential misuse of profiles or stored samples; innovations in extracting sensitive genetic information from one's forensic DNA profile; and the possibility of false accusations due to contamination, innocent presence, DNA transfer, or the like. But none of these possibilities appear on the waiver form given to defendants when they take the deal.[118]

Furthermore, even if the consent form did list these potential harms, individuals still may be unable to accurately envision these risks, as the assemblage of genetic databases is impossibly opaque.[119] Relatedly, individuals may lack incentives to take the request seriously.[120] Without an explanation of vivid risks or sufficient incentives to take the request

---

116. Roth, *supra* note 15, app. at 457.

117. *Id.* at 445 n.223 ("One database participant said that she tried to read the waiver form carefully but had to make a quick decision, and wanted to get out of the courthouse as quickly as possible. She found the form difficult to understand, but did not ask the judge or her attorney questions. . . . A college student did not read the waiver form at all before signing it.").

118. *Id.* at 444–45.

119. On consent-based regimes generally, Richards and Hartzog write that an explanation of *vivid* risks is a necessary precondition for consent:

> Informed consent regimes for data will only work if the risks are vivid. . . . [T]hese risks that we are being asked to waive through consent might materialize without our even knowing it. . . . Even when manifested, data harms often stay hidden. And our risk calculus is further funneled into wild speculation, paranoia, or overconfidence.

Richards & Hartzog, *supra* note 103, at 1495.

120. *Id.* at 1496. Incentives to take each request seriously are also a necessary precondition for consent:

> Requests for informed consent are, by definition, individualized and atomized. The moral weight of these frameworks is concentrated in the information delivered to the subject and the subject's voluntary execution of a legally significant choice. Through this call and response, people's autonomy is ostensibly respected, which can justify a host of actions that would otherwise be objectionable. But these justifications break down when people have little incentive to meaningfully consider what is being asked of them. This incentive can be diminished either because the stakes appear insignificant or because people cannot easily see how their decision is consequential because the relationship between the consent and the risks is too remote. Others simply have little incentive to take each request seriously because they feel powerless.

*Id.*

seriously, consent forms may actually be harmful to what little autonomy they purport to protect.[121]

Finally, even if it were possible to obtain uncoerced, fully informed consent, widespread consent-based DNA collection impermissibly erodes collective autonomy interests.[122] As genetic information has an inherently relational quality, one individual's choice to consent to DNA collection may compromise the genetic privacy of an unwitting third person, as seen in the case of investigative genetic genealogy.[123] It is reasonable to anticipate that many individuals will assign greater weight to the particular costs and benefits of consenting to DNA collection that are relevant to them and people like them.[124] "[W]hen [members of] majority groups consent to offers that are cost-benefit justified for themselves," the autonomy interests of marginalized groups may be compromised.[125] In considering regulating against DNA on Demand, legislators should take seriously this inconsentability problem.

### *2. Baseless Surveillance*

Another harm wrought by DNA overcollection is baseless surveillance. The Fourth Amendment generally requires a warrant supported by probable cause in order for a search to be legitimate.[126] Probable cause is premised on the idea "that *any* intrusion in the way of search or seizure is an evil, so that no intrusion at all is justified without a careful prior determination of necessity."[127] The Fourth Amendment warrant requirement protects individuals against "rash and unreasonable interferences with privacy and from unfounded charges of crime."[128] This central tenet of Fourth Amendment doctrine underlies the Supreme Court's decisions imposing limiting principles on exceptions to the warrant requirement. For example, in *Carpenter v. United States*, the case that recognized a limit on the third-party doctrine in the context of cellphone location data, the Court emphasized that the law must embody the Fourth Amendment's goals "to

121. "[W]ithout these preconditions, consent models for data practices risk being harmful and corrosive to the very autonomy they seek to protect." *Id.* at 1466.

122. Selinger and Hartzog make the same observation in the context of facial surveillance. *See* Selinger & Hartzog, *supra* note 104, at 50–51.

123. *See supra* note 85 and accompanying text.

124. Selinger and Hartzog make the same observation in the context of consenting to facial surveillance. *See* Selinger & Hartzog, *supra* note 104, at 51.

125. *See id.*

126. U.S. CONST. amend. IV.

127. Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971).

128. Brinegar v. United States, 338 U.S. 160, 176 (1949).

secure the privacies of life against arbitrary power" and "to place obstacles in the way of a too permeating police surveillance."[129]

Overcollection of DNA by police and permissive attitudes toward warrantless DNA collection contravene this command. Although probable cause is a famously flexible standard,[130] it at least requires a police officer's reasonable belief that either "an offense has been or is being committed,"[131] or that evidence of a crime will be found in the place searched,[132] and particularity with respect to "the place to be searched, and the persons or things to be seized."[133] When police conduct a search pursuant to a warrant requirement exception, these safeguards against arbitrary privacy intrusions are jettisoned. As discussed previously, no level of suspicion or degree of particularity is necessary in order for police to request an individual's consent to DNA collection.[134] Similarly, police may obtain thousands of genetic profiles from willing private firms with no probable cause or particularity because of the third-party doctrine, which has been uncritically applied to genetic data.[135] Finally, application of the abandonment doctrine to genetic data enables police to collect DNA from surfaces touched by individuals in an interrogation room or from discarded objects obtained by rummaging through trash, all without running afoul of the Fourth Amendment.[136]

This seemingly unflinching application of Fourth Amendment warrant exceptions to genetic data has enabled the baseless collection and indefinite surveillance of innocent individuals. In New York City, for example, the NYPD admitted that of the people represented in the City DNA index—which largely consists of genetic data collected through DNA dragnets and "abandoned" DNA collection—at least 25% have never been convicted of a crime, and 5% are children.[137] The law's permissive attitude toward DNA collection tactics produces the absurd outcome that innocent individuals

129. Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018) (citations and internal quotation marks omitted).

130. *See, e.g.*, Illinois v. Gates, 462 U.S. 213, 232 (1983) ("[P]robable cause is a fluid concept—turning on the assessment of probabilities in particular factual contexts—not readily, or even usefully, reduced to a neat set of legal rules.").

131. *Brinegar*, 338 U.S. at 175–76 (quoting Carroll v. United States, 267 U.S. 132, 162 (1925)).

132. Texas v. Brown, 460 U.S. 730, 742 (1983).

133. U.S. CONST. amend. IV.

134. *See supra* Section I.B.1.

135. *See supra* Section I.C.

136. *See* California v. Greenwood, 486 U.S. 35, 41 (1988) (quoting Katz v. United States, 389 U.S. 347, 351 (1967)) ("[W]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.").

137. Press Release, The Legal Aid Soc'y, After NYPD Acknowledges Almost 2,000 People Should Be Removed from City DNA Index, Legal Aid Calls on City Council to End Genetic Stop-and-Frisk (Oct. 15, 2020), https://legalaidnyc.org/wp-content/uploads/2020/10/10-15-20-After-NYPD-Acknowledges-Almost-2000-People-Should-be-Removed-From-City-DNA-Index-LAS-Calls-on-City-Council-to-End-Genetic-Stop-And-Frisk.pdf [https://perma.cc/9Z7B-TUK3].

experience greater intrusions on privacy than convicted criminals. As Erin E. Murphy writes:

> Oddly enough, a DNA sample collected from a known felon and uploaded to the FBI's national database enjoys far greater safeguards against misuse and abuse than does an innocent person's DNA when gathered by police on a hunch or on a whim. . . . [W]hen police collect the DNA sample . . . through a voluntary request or outright trickery—all these protections disappear. . . . Beyond the horizon lies a wild frontier in which a DNA sample is as easy to gather as a bottle from a trash barrel, databases are filled and searched according only to law enforcement whim, and the law has nothing to say about any of it.[138]

This illogical outcome is not inevitable. Litigators and scholars have advanced strong legal arguments as to why exceptions to the Fourth Amendment warrant requirement should not be applied in the context of genetic information.[139] Where the Court has not yet answered this call, legislators should step in to limit suspicionless DNA collection in order to safeguard privacy interests.

*3. Chilling Effects*

Genetic data maximalism has negative secondary effects, including the risk of chilling effects—disincentivizing valuable, pro-social behavior. For example, individuals may be less likely to voluntarily come to the police station to aid in a criminal investigation if they are worried about police officers later secretly collecting DNA from surfaces that they have touched, or that they will feel compelled to provide a DNA sample upon request. DNA overcollection may disincentivize not only willing participation in criminal investigations, but also civil rights and liberties. For example, fear of coercive or surreptitious DNA collection during a political protest may

138. MURPHY, *supra* note 21, at 168–69.

139. *See, e.g.*, Ram, *supra* note 81, at 1380–90 (arguing that *Carpenter*'s test supports a finding that individuals maintain an expectation of privacy in their genetic information, even when that information is conveyed to a third party); Brief for American Civil Liberties Union, American Civil Liberties Union of Iowa & Electronic Frontier Foundation as Amici Curiae Supporting Defendant-Appellant at 10, State v. Burns, 988 N.W.2d 352 (Iowa 2023) (No. 20-1150), https://www.eff.org/document/state-v-burns-iowa-supreme-court-eff-aclu-amicus-brief [https://perma.cc/P6GL-RNU7] (arguing that the abandonment doctrine is inappropriate as applied to surreptitious DNA collection because (1) individuals cannot avoid shedding DNA and hence do not voluntarily discard DNA when traces are left behind; (2) "sophisticated technology is required to extract genetic information from a sample;" and (3) due to the deeply personal nature of DNA, "the privacy interest in unavoidably shed DNA is of a different magnitude than the interest in physical items abandoned or placed in the trash").

disincentivize individuals from exercising their right to assembly.[140] The risk of chilling effects underscores the urgency of making combatting genetic data maximalism a policy priority for legislatures seeking to meaningfully safeguard privacy interests.

### *B. Harms from Overuse*

All too often, popular conceptions of privacy stop at the moment that human information is collected.[141] This "'secrecy paradigm'—the idea that privacy is only about keeping things hidden, and that information exposed to another person ceases to be private"—underlies the fatalist notion that privacy is dead.[142] Defining privacy in this way shrinks its significance and overlooks many privacy harms.[143] We should instead think about genetic information "not just at the time that it is collected and thus known but in terms of how it is used—its detection, collection, collation, correction, consultation, combination, adaption, alteration, organization, transformation, transmission, recording, retrieval, analysis, storage, structuring, encryption, decryption, disclosure, deletion, destruction, and erasure—for a start."[144] Accounting for the myriad ways that genetic information is used is therefore crucial to crafting meaningful safeguards to genetic privacy. Accordingly, this Section explores common privacy harms stemming from the overuse of DNA.

#### *1. Thwarted Expectations*

Many genetic privacy violations involve thwarted expectations about how individuals' genetic data will be used, searched, disclosed, and stored.[145] Thwarted expectations undermine autonomy interests, "because [they] result[] in people's inability to make choices in accordance with their

140. *See* Lauren Kirchner, *If I Go to a Protest, What Kinds of Personal Information Might Police Collect About Me?*, MARKUP (June 16, 2020, 1:00 PM), https://themarkup.org/the-breakdown/2020/06/16/if-i-go-to-a-protest-what-kinds-of-personal-information-might-police-collect-about-me [https://perma.cc/JH4K-UQAC] (discussing New York City Legal Aid attorneys' warnings that police may swab masks left behind at protests or manipulate children into providing DNA samples).

141. *See* NEIL RICHARDS, WHY PRIVACY MATTERS 27 (2022) ("All too often . . . popular legal conversations about privacy seem to stop at the moment our human information is collected.").

142. *Id.* (citing DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 42 (2004)).

143. *See id.* at 27–29 (discussing the flaws of the secrecy paradigm).

144. *Id.* at 26.

145. *See* Citron & Solove, *supra* note 24, at 849–53 (identifying thwarted expectations as a frequent symptom of privacy violations).

preferences."[146] Secondary effects, such as emotional harms, compound the damage done by thwarted expectations.[147]

Thwarted expectations about the use of genetic information frequently manifest when DNA collected for one purpose is used for another purpose.[148] For example, in the San Francisco rape kit case, the victim's DNA was collected as part of a medical examination, but was stored in a database that allowed for searches for criminal investigative purposes.[149] Doubtless, when the victim consented to DNA collection, it was "for a very specific purpose: to catch the person who raped [her],"[150] and it was not foreseeable that police would frictionlessly exceed the scope of that consent by including her genetic profile in a criminal database to be searched and stored indefinitely. The uniform condemnation of the San Francisco rape kit case is representative of the intuition that thwarted expectations are grave privacy harms.

Thwarted expectations arise in other contexts, too. For example, when police search newborn public health screening databases in criminal investigations, they deviate from the purpose for which the DNA was given—to screen for medical conditions.[151] Similarly, when individuals consent to routine medical testing such as pap smears, it is understandable that they would feel "violated," if, for example, police secretly obtain their genetic profile from the resulting medical waste in order to investigate their father for a crime that ultimately sends him to jail for life.[152] Individuals who consent to DNA collection in a DNA dragnet may not expect that their sample will not only be used in the criminal investigation for which they provided the sample, but will be stored and searched indefinitely in a "Suspect Index."[153] Finally, individuals who take commercial genetic tests and upload their information to GEDMatch to learn about their ancestry may be surprised to learn that their genetic information may be searched by

146. *Id.* at 849.

147. *Id.*

148. *Id.* (describing thwarted expectations as "the undermining of people's choices, such as breaking promises made about the collection, use, and disclosure of personal data.").

149. *See* Paybarah, *supra* note 1.

150. *Id.*

151. *See* Mullin, *supra* note 11; *California Stores DNA from Every Baby*, *supra* note 12.

152. *See* MURPHY, *supra* note 21, at 169.

> On the campus of a state university at the turn of the millennium, a young college student goes to the health clinic. As part of the examination, she is given a pap smear to test for cellular abnormalities. Little does she know that the sample is saved, in accordance with a law that requires preservation in the event of later malpractice suits. Even less might she anticipate that, not even five years later, police will obtain the sample without her knowledge, an act she will later describe as leaving her feeling "violated." It will be DNA culled from that sample that eventually sends her father to jail for life.

*Id.*

153. *See supra* note 16 and accompanying text.

police to investigate them or their relatives for a crime, even if they have not opted into law enforcement access.[154]

Thwarted expectations about how collected DNA will subsequently be used, stored, and searched frequently arise in many different contexts, irrespective of particular database types or search methods. The harm is severe, and frequently pernicious, as the public typically does not learn of the ways in which their expectations have been thwarted unless police rummaging yields a match;[155] and even then, the particular databases or methods used may be within a black box.[156] Crafting legislation that only addresses specific types of searches leaves the door open for other avenues for thwarted expectations. Accordingly, it is imperative that legislators craft regulations to prevent thwarted expectations before they occur.

*2. Chilling Effects*

Just as overcollection of genetic information risks chilling socially beneficial behavior, so too does the overuse of genetic information. For example, in the wake of the San Francisco rape kit case, advocacy groups were rightly concerned that news of using rape kit DNA to implicate victims in subsequent crimes would lead to lower sexual assault reporting rates and lower participation rates in medical examinations, which can be essential in criminal prosecutions.[157] Similarly, police usage of newborn medical screening databases threatens to undermine crucial public health programs.[158] These chilling effects tend to go hand-in-hand with thwarted expectations, which compounds the harm to autonomy interests. To meaningfully safeguard privacy interests, legislation must therefore take these weighty secondary effects into account.

154. *See supra* note 83 and accompanying text.

155. *See* MURPHY, *supra* note 21, at 170.

> [I]t was only because the pap smear led to a match that we know that police had rummaged through the daughter's medical waste. If law enforcement's hunch had proven wrong, it is likely the public would never have learned that a pap smear had been accessed, tested, and typed. Indeed, we still do not know whether [that] DNA [sample] was the only sample surreptitiously collected in connection with that case, or whether police quietly accessed one or ten or one hundred samples before aligning on hers.

*Id.*

156. *See* Murphy, *supra* note 10 (describing the University of Idaho homicide investigation affidavit's "thoughtful omission" of any reference to investigative genetic genealogy).

157. *See, e.g.*, RAINN, *supra* note 4.

158. *See* Ram, *supra* note 81, at 1306.

*3. Indefinite, Large-Scale Surveillance*

Not only is genetic surveillance often baseless,[159] but it is also often indefinite, because local law enforcement is free to set their own parameters for retention and expungement.[160]

Indefinite surveillance is a harm in itself, compounded by the harm flowing from suspicionless collection. The baffling result is that innocent individuals are frequently subject to greater intrusions on privacy than convicted criminals whose genetic profiles are retained in the national database and therefore subject to CODIS expungement requirements.[161] This directly contravenes the Fourth Amendment's underlying guarantees "to secure the privacies of life against arbitrary power" and "to place obstacles in the way of a too permeating police surveillance."[162]

Moreover, because of unconstrained collection practices and creative search methods such as investigative genetic genealogy, genetic surveillance is large-scale. Owing to the inherently relational nature of genetic information, even if a particular individual's DNA has not been collected, they may nevertheless be identified through relatives as distant as third cousins whose genetic information has been collected.[163]

The stakes of large-scale, indefinite, suspicionless surveillance are high. Surveillance "can chill the exercise of civil liberties," and impose a "power dynamic between the watcher and the watched" which "creates the risk of a variety of harms, such as discrimination, coercion, and the threat of selective enforcement."[164] As such, combatting indefinite, large-scale genetic surveillance must be a policy priority for legislators.

---

159. *See supra* Section II.A.2.

160. *See* Kreag, *supra* note 20, at 1503 ("[L]ocal law enforcement is free to set its own protocols for including and searching partial DNA profiles in their databases and for expunging DNA records.").

161. *See supra* note 138 and accompanying text.

162. Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018) (citations and internal quotation marks omitted).

163. As a 2018 study showed:

> 60 percent of Americans of Northern European descent—the primary group using [sites such as 23andMe and Ancestry.com]—can be identified through such databases whether or not they've joined one themselves . . . . Within two or three years, 90 percent of Americans of European descent will be identifiable from their DNA . . . .

Heather Murphy, *Most White Americans' DNA Can Be Identified Through Genealogy Databases*, N.Y. TIMES (Oct. 11, 2018), https://www.nytimes.com/2018/10/11/science/science-genetic-genealogy-study.html [https://perma.cc/ACK9-ZJM9] (citing Yaniv Erlich, Tal Shor, Itsik Pe'er & Shai Carmi, *Identity Inference of Genomic Data Using Long-Range Familial Searches*, 362 SCIENCE 690 (2018)).

164. *See* Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1935 (2013).

*4. Data Breaches*

Underregulation of DNA databases makes individuals susceptible to data breaches. For example, GEDMatch experienced a data breach in 2020 which overrode existing user settings, making all profiles visible to law enforcement for the duration of the breach.[165] This means that despite the efforts of commercial DNA databases like GEDMatch to enact more privacy-protective policies, users' genetic data has nevertheless been unwillingly exposed to third parties. Similarly, because state and local databases are not subject to the same data security requirements as CODIS, they too pose a risk to the many individuals whose genetic information is stored therein.[166]

A breach of a biometric database is an exceptionally bad data breach—you can change a password, but you can't change your DNA. Genetic information is also a particularly sensitive type of personal data, as it can reveal a wealth of information about an individual's health, familial relationships, and identity. Individuals whose sensitive data is exposed in a data breach suffer harms in the form of increased risk and anxiety.[167] Any regulation of DNA on Demand must account for the risk of data breaches and the tangible harms that flow from breaches of sensitive genetic information.

## III. DESIGNING HARMS-CENTERED SAFEGUARDS

There is a political appetite for genetic privacy. For example, recent state laws passed in Maryland and Montana regulate forensic genetic genealogical DNA searches.[168] California passed a state law providing procedures for "reference sample" DNA, such as those DNA samples collected from victims or other individuals for the purpose of exclusion, in response to the San Francisco rape kit case outrage.[169]

However, in the present reality where police have a myriad of databases and collection methods at their disposal, regulations that are tailored toward specific database types or collection tactics are doomed to be fatally underinclusive and will fail to prevent the severe privacy harms wrought by DNA on Demand. Furthermore, these laws reduce privacy protection to a

165. Murphy, *supra* note 74.

166. *See* Kreag, *supra* note 20, at 1544–45.

167. *See* Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737, 756–74 (2018) (demonstrating that victims of data breaches experience cognizable harms of increased risk and anxiety).

168. *See* Lynch, *supra* note 23.

169. *See* Nicole Wetsman, *Rape Kit DNA Protected Under a New California Law*, VERGE (Oct. 3, 2022, 4:05 PM), https://www.theverge.com/2022/10/3/23384969/rape-kit-survivor-dna-protected-california [https://perma.cc/QPX7-LV5Z].

mere procedural exercise without a clear sense of which values guide the interpretation and implementation of the law. In other words, their primary focus is on whether procedures for DNA collection and use have been followed, rather than whether that DNA collection and use is an unreasonable interference with privacy.[170]

In order to meaningfully safeguard genetic privacy, it is imperative that lawmakers enact laws oriented toward combatting the most severe harms that flow from the overcollection and overuse of DNA in criminal investigations. To that end, this Part offers several substantive limits that will prevent harms to genetic privacy across contexts.

### *A. Limits on Collection*

Jurisdictions should enact regulations that target the most significant harms posed by DNA overcollection. Some of the most severe genetic privacy harms, including coerced or unwitting consent, baseless surveillance, and chilling effects, have roots in the overcollection of DNA.[171] Accordingly, jurisdictions should enact regulations that target these harms from overcollection.

First, collection of DNA pursuant to "consent" should be banned in highly coercive environments, such as traffic stops, sidewalk detentions, home searches, plea bargains, and any other encounters with police or prosecutors where a reasonable person would not feel free to leave.[172] Experience has shown that nearly everyone will consent to a request to consent to search, and that consent searches are highly susceptible to racial bias.[173] To that end, they should be banned.

Second, collection of DNA pursuant to "consent" in less coercive environments—and subsequent use of that genetic information—should be narrowly tailored to the scope of the permission given.[174] Given that people such as crime victims may have a genuine interest in letting police collect

---

170. The tendency of genetic privacy laws to have a fatally procedural focus echoes a common problem with privacy law generally. *See generally* Neil Richards & Woodrow Hartzog, *A Duty of Loyalty for Privacy Law*, 99 WASH. U. L. REV. 961, 1002 (2021) ("[F]air information practices of notice, choice, consent, access, etc. . . . frequently reduce privacy frameworks into mere procedural exercises."); Woodrow Hartzog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. REV. 1687, 1691, 1696 (2020) (discussing privacy law's focus on procedural rules at the cost of more substantive protections) ("Procedural requirements like obligations to get peoples' consent for data practices ultimately normalize the kinds of data collection and surveillance harms that they are supposed to mitigate.").

171. *See supra* Section II.A.

172. This suggestion echoes a proposal by the Electronic Frontier Foundation to ban consent searches of all kinds in high-coercion settings. *See* Schwartz, *supra* note 106.

173. *See supra* notes 105–14 and accompanying text.

174. This suggestion echoes a proposal by the Electronic Frontier Foundation to strictly limit consent searches of all kinds in less coercive settings. *See* Schwartz, *supra* note 106.

their DNA for investigative purposes, consent searches should be allowed in some circumstances. However, any subsequent use of that genetic information must not exceed the scope of the consent for which it was given, and strict procedural requirements governing storage of the genetic information must be followed.[175] Regulating this aspect of DNA overcollection would prevent thwarted expectations about how collected DNA will later be used, and in turn reduce the risk of chilling behavior that may be beneficial to crime victims and society.

Third, suspicionless collection of DNA should be banned. The suspicionless collection of DNA contravenes the Fourth Amendment command that "no intrusion at all is justified without a careful prior determination of necessity."[176] Banning suspicionless collection of DNA guards against discriminatory enforcement and the risk of chilling civil liberties.[177]

### *B. Limits on Use and Retention*

Jurisdictions should also tailor regulations to preventing the most grave harms wrought by law enforcement overuse and mishandling of genetic data.

First, DNA given for one purpose should not be used for another purpose. Thwarted expectations can be one of the most violative privacy harms, so it is only logical for laws to be oriented toward preventing this type of harm.[178] Banning this manner of DNA use would serve as a substantive safeguard against the harms flowing from thwarted expectations, as opposed to merely banning particular types of searches or imposing warrant requirements, which are mere procedural requirements that are easily thwarted thanks to underinclusive laws.[179]

Second, states should embrace the principle of data minimization[180] when crafting regulations regarding DNA storage in order to guard against

175. Although procedural requirements are not sufficient to safeguard genetic privacy, *see supra* note 170 and accompanying text, regulations may benefit from procedural limitations so long as they are tailored toward preventing privacy harms from DNA overcollection and overuse. Because many legislatures have come to procedural solutions such as warrant requirements on their own, they are not the focus of this proposal, but they should be considered as part of a larger regulatory scheme.

176. Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971).

177. *See* Schwartz, *supra* note 106.

178. *See supra* Section II.B.1.

179. Again, procedural limitations such as warrant requirements or bans on particular types of searches may be helpful, but are not sufficient absent a larger regulatory scheme oriented toward preventing privacy harms. As such, these procedural requirements are not the focus of this proposal. *See supra* note 175 and accompanying text.

180. *Principle (c): Data Minimisation*, INFO. COMM'R'S OFF., https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles

baseless surveillance and reduce risk of harm from data breaches. To this end, states should limit the type of data that is retained in state and local databases. For example, when DNA is given for identification or exclusion purposes, it should be destroyed and the information deleted immediately after a search is run. This would strike the right balance between an individual's genetic privacy and the government's interest in identification,[181] or victims' interests in solving crime. States should also limit the type of DNA stored in state and local databases to DNA collected from violent crime scenes. If agencies maintain other DNA databases—such as victim DNA databases—regulations should expressly prohibit the inclusion of that genetic data in the crime-solving genetic database, so as to avoid the risk of thwarted expectations and chilling effects on crime reporting and participation in investigations.[182] Furthermore, states should outline clear expungement requirements. Genetic profiles of convicted offenders must be deleted if their conviction has been overturned. If states or localities maintain genetic profiles of arrestees for longer than the time required to identify the individual, then they must be deleted if the arrestees are acquitted, their charges are dismissed, or no charges are filed within the applicable time period.

### *C. Oversight and Security*

Finally, regulations should stipulate oversight mechanisms and robust data security practices. All state and local databases must be subject to independent oversight and regular audits, such as those required by CODIS.[183] State and local databases should have—at minimum—the same security requirements as CODIS.[184] However, recent scholarship on how to best prevent and reduce the harm of data breaches suggests that a more holistic approach to data security—by embracing practices such as data minimization, data mapping, and requiring certain defaults—may be a more auspicious approach.[185]

---

/the-principles/data-minimisation/ [https://perma.cc/HYF9-F2ZS]. The data minimization principle states that data holders should "identify the minimum amount of personal data [they] need to fulfil [their] purpose," and "hold that information, but no more." *Id.*

181. In *Maryland v. King*, 569 U.S. 435 (2013), the identification value of DNA largely motivated the Court's allowance of DNA collection from individuals who were arrested, but not yet convicted. *King*'s dictates can still be followed while minimizing intrusions to genetic privacy by expunging the information once it has ostensibly been used for identification purposes.

182. *See supra* Sections II.B.1, 2.

183. *See supra* Section I.A.1.

184. *See supra* Section I.A.2.

185. DANIEL J. SOLOVE & WOODROW HARTZOG, BREACHED! 193–97 (2022) ("[L]awmakers can use various hard and soft nudges to promote or discourage activities. One such way is to require certain defaults. Defaults can be overridden by user choices, but how they are set has tremendous influence. . . .

## IV. POTENTIAL OBJECTIONS

Naturally, there are several potential objections to the approach advanced by this Note. This Part anticipates and addresses some of those objections.

### *A. Too Broad*

It is reasonable to assume that many people share the legislature's instinct that particularly egregious *types* of database searches or *methods* of DNA collection should be regulated against. In other words, there may be good reason to treat different types of databases or collection practices differently. The intuition that laws should be narrowly tailored in order to avoid impinging on competing interests—such as the efficient investigation of violent crimes—is undoubtedly correct, but the problem is that legislatures have consistently misidentified the appropriate ends to be achieved by regulation. Laws that are restricted to limiting particular collection methods or database searches miss the forest for the trees, regulating procedure for procedure's sake rather than regulating toward the more urgent and fundamental objective of preventing privacy harms. By centering the legislative discussion around the prevention of privacy harms wrought by overuse and collection, laws can be narrowly tailored toward achieving the appropriate end.

### *B. Costs to Crime-Solving Are Not Worth It*

Another anticipated objection to this proposal is that society's interest in crime deterrence and investigation is simply too important, and the societal costs of making this task ostensibly more difficult are not worth incurring. Undoubtedly, crime victims and the public at large have a high interest in solving crimes and promoting safety and security. But the Fourth Amendment has always demanded a balancing of this interest against civil liberties, ever since the Founders recognized and "reviled" the "evils" of unconstrained government searches and surveillance.[186] Moreover, the

---

There are many components of privacy regulation that can strengthen security, such as data minimization, data mapping, and other requirements. Good privacy hygiene can reduce the likelihood of breaches as well as their severity.").

186. Riley v. California, 573 U.S. 373, 403 (2014) ("[T]he Fourth Amendment was the founding generation's response to the reviled 'general warrants' and 'writs of assistance' of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity."); Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971) ("[A]ny intrusion in the way of search or seizure is an evil, so that no intrusion at all is justified without a careful prior determination of necessity . . . those searches deemed necessary should be as limited as possible. Here, the specific evil

decentralized assemblage of DNA databases, combined with variations in the quality of collection, search, and storage methods may actually lend itself to *inefficiencies* in crime solving in the form of backlogs, missing evidence, and wrongful convictions.[187] Finally, the goal of regulating against DNA overcollection and overuse is not to make it *impossible* for police to obtain or use genetic information in criminal investigation, but to introduce modest transaction costs so as to disincentivize broad, suspicionless surveillance, thereby "eliminat[ing] the specter of a surveillance state because it would be resource intensive."[188] Introducing these meager transaction costs to the currently frictionless system in the form of sensible substantive protections targeted to prevent privacy harms would strike the appropriate balance between individual liberties and legitimate law enforcement and security needs.

### *C. Genetic Surveillance Is No Big Deal*

Finally, there is the notion that genetic surveillance is no big deal. This objection takes the shape of the familiar Privacy Is Dead myth or the Nothing To Hide argument.[189] Both of these notions are flawed and harmful to collective autonomy interests. As Neil Richards writes:

> The Privacy Is Dead idea is false on its own terms. Our technologies collect lots of personal information, but lots of things are still private. We still wear clothes to cover our naked bodies; we still lock the doors to our homes (and our bedrooms and our bathrooms); we still keep secrets; and we still care about privacy. . . . We live in a society in which information is power, and "privacy" is the word we use to talk about the struggles over personal information, personal power,

is the 'general warrant' abhorred by the colonists, and the problem is not that of intrusion per se, but of a general, exploratory rummaging in a person's belongings.").

187. *See* MURPHY, *supra* note 21, at 266–82 (describing how lack of regulation surrounding forensic DNA collection and use has led to a myriad of inefficiencies in crime solving and criminal justice).

188. Hartzog & Selinger, *supra* note 24, at 1383; *see also id.* at 1369 (emphasizing how a focus on obscurity in the form of transaction costs can "accommodate multiple interests in reforming surveillance law, making consensus more likely").

189. Neil Richards describes the Privacy Is Dead myth as the pervasive idea among academics, public commentators, and industry leaders that because "[w]e live in a society that constantly generates vast quantities of human information" which is "tracked, screened, and sorted by corporations and governments and shared exponentially to others," privacy is dead. *See* RICHARDS, *supra* note 141, at 1. Richards describes the Nothing To Hide argument as "the idea that privacy is no more than the ability to hide unpleasant truths about ourselves from the public, and that if we have no unpleasant truths to hide, we don't need privacy." *Id.* at 72.

> and personal control. If we think of it this way, privacy is very much alive—but very much hanging in the balance.[190]

The Nothing to Hide argument shares the same problems, and suffers from the additional flaw that it "focuses narrowly on privacy as an individual matter rather than as a social value."[191] Genetic information is inherently relational, and individual genetic surveillance may compromise collective autonomy interests, or the autonomy interests of other individuals. This harm is particularly severe when members of majority groups consent to offers that are cost-benefit justified for themselves but that compromise autonomy interests of marginalized groups.[192] An additional flaw of the Nothing To Hide argument is that what one may not feel the need to hide one day may become criminal the next. Given the recent criminalization of abortion in several states, this is a very real risk.[193]

## CONCLUSION

As stories of questionable DNA collection and search methods by police continue to make the headlines, more public attention is being given to seemingly limitless law enforcement access to our most intimate and sensitive information. Recent state laws targeting particular types of DNA database searches or particular DNA collection methods evince a political will for genetic privacy protection, but are likely to be ineffective against the wide variety of DNA collection techniques that police have at their disposal, or against the vast assemblage of genetic data repositories that police may search and frictionlessly move between if access to one particular database type is shunted. Accordingly, to prevent the harms wrought by genetic privacy invasions, the law must be oriented toward combatting genetic data privacy violations across all types of DNA collection and use. By centering the discussion around the privacy harms wrought by DNA overcollection and overuse, the law can overcome its strictly procedural focus and move toward substantive and meaningful limits on law enforcement access to and use of genetic information. Only

190. RICHARDS, *supra* note 141, at 2.

191. *Id.* at 76.

192. *See supra* notes 124–25 and accompanying text.

193. After the Court ruled in *Dobbs v. Jackson Women's Health Organization* that "the [federal] Constitution does not confer a right to abortion . . . and the authority to regulate abortion must be returned to the people and their elected representatives," several states banned almost all abortions. 142 S. Ct. 2228, 2279 (2022). As of March 2023, abortions are banned in fourteen states, and the future of abortion rights in many other states remains uncertain. *Tracking the States Where Abortion Is Now Banned*, N.Y. TIMES (July 24, 2023, 5:00 PM), https://www.nytimes.com/interactive/2022/us/abortion-laws-roe-v-wade.html [https://perma.cc/DEY6-EYG8].

by appreciating and legislating against these harms may we repudiate the DNA on Demand regime.

Emma Kenny-Pessia*

* J.D. Candidate (2024), Washington University School of Law; B.A. (2019), Barnard College. My deepest gratitude to Professor Neil Richards for inspiring me to write on a topic in privacy law, and for providing guidance throughout. I am also indebted to the editors of the *Washington University Law Review* for their suggestions and editing efforts. Finally, thank you to my family and friends for their unwavering love and support.