Brooklyn Law Review

Volume 87
Issue 4 *SYMPOSIUM: THE ROLE OF THE "VICTIM" IN THE CRIMINAL LEGAL SYSTEM*

Article 12

5-25-2022

DNA Dystopia: How the National Security Apparatus Could Map the Entire Genome of America Without Violating the Fourth Amendment or the Constitutional Right to Privacy

Elias Rios III

DNA Dystopia

HOW THE NATIONAL SECURITY APPARATUS COULD MAP THE ENTIRE GENOME OF AMERICA WITHOUT VIOLATING THE FOURTH AMENDMENT OR THE CONSTITUTIONAL RIGHT TO PRIVACY

INTRODUCTION

At-home genetic tests like 23andMe and DNAncestry are popular stocking stuffers for parents, a novel test to see where your family hails from, or even a way to gain information to make informed health care decisions based on genetic risk factors.[1] The terms of service for these products often state that the testing databases' rights and obligations to customers' information can be freely assigned away, which poses the potential issue of other companies acquiring the rights to your genetic information.[2] In addition to these testing databases, there are third-party websites, databases, and services that a person can sign up for that can utilize your genetic information in different ways.[3] Today's data or credit card breach perpetrated by a foreign hostile actor[4] could easily become tomorrow's breach of genetic information to be used by nefarious actors.[5]

---

[1] *DNA Reports List*, 23ANDME, https://www.23andme.com/dna-reports-list/ [https://perma.cc/YF5E-6UQ4] (listing available reports and services: ancestry composition, "Neanderthal Ancestry," family tree services, "trait reports" including early hair loss, and "Health + Ancestry Service[s]" including "[h]ealth [p]redisposition [r]eports" for such genetic risks as "nerve and heart damage," autoimmune disorders, "Type 2 diabetes," and certain forms of cancer).

[2] *See Terms of Service*, 23ANDME (Sept. 30, 2019), https://www.23andme.com/about/tos/ [https://perma.cc/XEV6-TJ5C]; *Ancestry Terms and Conditions*, *2.2.3 Ownership of Your Content*, ANCESTRY (Aug. 3, 2021), https://www.ancestry.com/cs/legal/termsandconditions#ownership-of-content [https://perma.cc/NX76-PVAD].

[3] *See* Tomohiro Takano, *The 17 Best DNA Upload Sites for Additional Analysis on Raw DNA Data File in 2021—Including Free Ones! (For 23andMe, AncestryDNA, MyHeritage Users)* (Sept. 20, 2021), https://blog.genomelink.io/posts/best-raw-dna-data-upload-sites [https://perma.cc/CWM6-WD4L] (providing brief introductions to seventeen different third-party DNA sites that allow users to upload data to further analyze genetic information in categories like "Ancestry Test and Family Tree Services," "Contribute to Science," and "Nutrition and Fitness").

[4] *See* Allen St. John, *Justice Department Charges Chinese Nationals with Equifax Data Breach*, CONSUMER REPS. (Feb. 10, 2020), https://bit.ly/3NqIDEz [https://perma.cc/D58V-46SB] (stating that "[t]he 2017 hack compromised the personal data of 145 million Americans").

[5] *See* Dan Rafter, *Is Your DNA Info Safe From Data Breaches, and What Are the Privacy Concerns?*, NORTON, https://nr.tn/3GcCYQb [https://perma.cc/S674-MNDH] (describing scenarios where DNA data could be used by hackers or exposed on the dark web).

National security threats are not always readily apparent, nor do they always seem intuitive.[6] On December 20, 2019, the US Department of Defense added direct-to-consumer (DTC) deoxyribonucleic acid (DNA) testing to the growing list of national security threats on the horizon.[7] In their 2019 memorandum, Under Secretary of Defense for Intelligence Joseph D. Kernan and acting Under Secretary of Defense for Personnel and Readiness James N. Stewart stated that the largely unregulated testing industry risked inadvertent exposure of genetic information to adversaries.[8] The memorandum also noted that these adversaries may be able to exploit the unregulated DNA data to conduct mass surveillance, thereby creating operational security risks.[9]

Over the past fifty years, mass surveillance within the United States and abroad has laid bare the fundamental tension between ensuring national security and the preservation of civil liberties in the face of overreach by intelligence-gathering organizations.[10] In 1974, a report from *The New York Times* unmasked a series of internal reports of the Central Intelligence Agency (CIA), detailing surveillance operations against antiwar protestors and other Americans.[11] In response to reports of government overreach in domestic surveillance, a Senate Select Committee was created to study intelligence activities.[12] Between 1953 and 1973, the Committee found that the CIA built a computerized index of nearly 250,000 entries based on intercepting, opening, and photographing first class letters.[13] "[B]etween 1969 and 1973," the Internal Revenue Service initiated tax investigations based on political considerations instead of tax criteria."[14] Political

---

[6] *See* Makena Kelly, *TSA Bans Employees from Using TikTok*, THE VERGE (Feb. 24, 2020, 10:07 AM), https://www.theverge.com/2020/2/24/21150667/tsa-tiktok-employee-ban-bytedance-chuck-schumer-homeland-security [https://perma.cc/MR38-AT8T] (explaining the Transportation Security Administration (TSA) banned the use of mobile app TikTok by employees after reports that TSA employees used the app to "explain[ ] some of the agency's boarding processes and rules").

[7] *See* Memorandum from Office of the Secretary of Defense to Department of Defense Personnel (Dec. 20, 2019) (advising military personnel against using DTC DNA testing due to the potential of "unintended security consequences and increased risk to the [Department of Defense] and mission").

[8] *Id.*

[9] *Id.*

[10] Adam R. Pearlman & Erick S. Lee, *National Security, Narcissism, Voyeurism, and Kyllo: How Intelligence Programs and Social Norms Are Affecting the Fourth Amendment*, 2 TEX. A&M L. REV. 719, 722 (2015).

[11] *Id.* at 748 (citing Seymour M. Hersh, *Huge C.I.A. Operation Reported in U.S. Against Antiwar Forces, Other Dissidents in Nixon Years*, N.Y. TIMES (Dec. 22, 1974), https://www.nytimes.com/1974/12/22/archives/huge-cia-operation-reported-in-u-s-against-antiwar-forces-other.html [https://perma.cc/UDD3-YFH5]).

[12] STEPHEN DYCUS ET AL., NATIONAL SECURITY LAW 612 (7th ed. 2020); S. REP. NO. 94-755 (1976).

[13] S. REP. NO. 94-755, at 6.

[14] *Id.* at 6–7.

leaders like Martin Luther King Jr. were investigated as "[c]ommunist 'sympathizer[s]'" using a "guilty until proven innocent" philosophy.[15]

In response to these issues, Congress passed the Foreign Intelligence Surveillance Act of 1978 (FISA), "which, among other things, created the Foreign Intelligence Surveillance Court ('FISC') to oversee government surveillance of wire communications."[16] The Fourth Amendment of the US Constitution ensures:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[17]

In conducting foreign intelligence surveillance, a warrant compliant with the Fourth Amendment is not required.[18] Additionally, it must be shown that the primary purpose of surveillance is for foreign intelligence reasons.[19] Thereafter, criminal defendants would challenge a prosecutor's use of evidence gathered pursuant to a FISA order, but without a warrant, as a violation of the Fourth Amendment's general warrant requirement.[20] To comply with these limitations, the DOJ compartmentalized its investigations.[21] After the September 11 terrorist attacks in 2001, this "wall" between domestic and foreign surveillance was smashed, as the congressional 9/11 Commission detailed how failures of the intelligence community[22] coincided with the passage of national security legislation like the PATRIOT Act.[23]

---

[15] *Id.* at 7. The report further describes instances of informants infiltrating the Women's Liberation Movement, the NAACP, and "sending agents to a Halloween party for elementary school children in Washington, D.C., because they suspected a local 'dissident' might be present." *Id.* at 7–8.

[16] Pearlman & Lee, *supra* note 10, at 748.

[17] U.S. CONST. amend. IV.

[18] United States v. Truong Dinh Hung, 629 F.2d 908, 912–13 (4th Cir. 1980).

[19] *Id.* at 913; *see also In re* Sealed Case, 310 F.3d 717, 726 (FISA Ct. Rev. 2002) (discussing the adoption of the "primary purpose" test in other circuits).

[20] Pearlman & Lee, *supra* note 10, at 751.

[21] *See* U.S. DEP'T OF JUST., OFF. OF THE INSPECTOR GEN., A REVIEW OF THE FBI'S HANDLING OF INTELLIGENCE INFORMATION RELATED TO THE SEPTEMBER 11 ATTACKS (UNCLASSIFIED VERSION) 24 (2006), http://fas.org/irp/agency/doj/oig/fbi-911/ [https://perma.cc/E2HC-VYSE] (see Chapter 2, Background; "The Criminal Division and FBI Headquarters made the policy decision about when to involve the [US Attorney's Office] in the investigation, since consulting with the USAO was viewed as a bright line signifying the transition from an intelligence investigation to a criminal investigation . . . . [D]uring this time period, no formal written guidelines governed the contacts between the FBI and the Criminal Division.").

[22] *Id.* The DOJ Office of the Inspector General concluded that due to the wall, in August 2001, an FBI agent in the New York Field Office was unable to participate in the criminal investigation of two 9/11 hijackers once the agent realized the two men had entered the United States. *Id.*

[23] Pearlman & Lee, *supra* note 10, at 754.

The US national security apparatus subsequently prosecuted its "War on Terror" without an effective "wall" between foreign and domestic intelligence collection procedures.[24] In 2013, the *Guardian* reported that the National Security Agency (NSA) was collecting phone records of millions of Verizon customers.[25] Over the next several months, the public learned that the NSA used the FISA courts to gain access to these telephone records, and operated a program called PRISM that collected data through back doors into companies like Google and Facebook.[26] The leaker of this information, Edward Snowden, was believed to have acquired over 1.5 million files from the NSA while working as a contractor.[27] The NSA's mass surveillance program was contemporaneously described as "a haystack-before-the-needle approach to information gathering."[28]

Recently, the US Court of Appeals for the Ninth Circuit ruled that the NSA's "metadata collection program exceeded the scope" of their congressional authorization.[29] The Snowden leaks and the national security litigation flowing from the activities related to mass surveillance reveal the depth, sophistication, and capabilities of government entities that engage in metadata collection under the auspices of national security.[30] In addition, this behavior illustrated how during the War on Terror, the lack of a "wall" infringed on the civil liberties of millions of Americans.[31] This note argues that genetic information recovered from DTC DNA tests and third-party DNA databases could be an area ripe for exploitation in the realm of mass surveillance by government entities, given the history of the government misusing their surveillance abilities and liberal

---

[24] *See* James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES (Dec. 16, 2005), https://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html [https://perma.cc/L9C5-XL2K] ("The previously undisclosed decision to permit some eavesdropping inside the country without court approval was a major shift in American intelligence-gathering practices, particularly for the National Security Agency, whose mission is to spy on communications abroad.").

[25] Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, GUARDIAN (June 6, 2013), https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order [https://perma.cc/3SGR-D9SV].

[26] Paul Szoldra, *This Is Everything Edward Snowden Revealed in One Year of Unprecedented Top-Secret Leaks*, BUS. INSIDER (Sept. 16, 2016), https://www.businessinsider.com/snowden-leaks-timeline-2016-9 [https://perma.cc/9H3G-R73V].

[27] *Id.*

[28] Stephen I. Vladeck, *Big Data Before and After Snowden*, 7 J. NAT'L SEC. L. & POL'Y 333, 334 (2014).

[29] United States v. Moalin, 973 F.3d 977, 996 (9th Cir. 2020).

[30] *See* Am. C.L. Union v. Clapper, 785 F.3d 787, 793 (2d Cir. 2015) ("We must confront the question whether a surveillance program that the government has put in place to protect national security is lawful . . . . As in the 1970s, the revelation of this program has generated considerable public attention and concern about the intrusion of government into private matters.").

[31] Pearlman & Lee, *supra* note 10, at 719.

discretion that courts have afforded the government's surveillance activities in the past.[32] Because the acquisition of DNA information from an individual has the potential to impact relatives both near and distant, new judicial remedies, constitutional protections, or federal legislation may be necessary to protect genetic privacy.[33] These legal protections for genetic data should be seriously considered before the moment of critical mass occurs: when the entire genetic map of America is sequenced and exploitable.

Part I of this note briefly explains how DNA is an incredibly valuable personal identifier,[34] how it is used in many facets of American society, and how DTC DNA tests have brought about a fundamental transformation in criminal investigations through DNA's ability to identify persons with unprecedented precision.[35] Part II assesses whether or not the widespread availability of genetic information is a national security threat, and if so, in what instances can it be weaponized.[36] Part III discusses the dangers of moving forward in integrating the acquisition of genetic information into the national security apparatus, because the types of high tech, data-driven surveillance campaigns conducted are notoriously difficult for courts to adjudicate[37] without favoring the intelligence gatherers and dismissing for lack of Article III standing.[38] Because my analysis leads to the designation that DNA data is not a widespread national security threat, Part IV explores what civil liberties could be endangered by designating DNA data as a national security threat and potential remedies. Finally, Part V surveys potential remedies and their pitfalls.

I. DTC TESTING AND OPEN-SOURCE DATABASES

DNA "is the hereditary material found in humans and almost all other organisms."[39] DNA is made up of four chemical

---

[32] *NSA Surveillance*, AM. C.L. UNION (Jun. 21, 2016), https://www.aclu.org/issues/national-security/privacy-and-surveillance/nsa-surveillance [https://perma.cc/6KUF-W8UV].

[33] Christine Guest, Comment, *DNA and Law Enforcement: How the Use of Open Source DNA Databases Violates Privacy Rights*, 68 AM. U. L. REV. 1015, 1042 (2019).

[34] *What Is DNA?*, MEDLINEPLUS, https://medlineplus.gov/genetics/understanding/basics/dna/ [https://perma.cc/Q6ZV-NGSJ].

[35] *See* Guest, *supra* note 33, at 1042.

[36] Sui-Lee Wee, *China Is Collecting DNA From Tens of Millions of Men and Boys, Using U.S. Equipment*, N.Y. TIMES (June 17, 2020), https://www.nytimes.com/2020/06/17/world/asia/China-DNA-surveillance.html [https://perma.cc/7KV7-V29M].

[37] Margaret B. Kwoka, *The Procedural Exceptionalism of National Security Secrecy*, 97 B.U. L. REV. 103, 121–25 (2017).

[38] *See* Klayman v. Obama, 759 F. App'x 1, 4 (D.C. Cir. 2019) (affirming dismissal of suit because appellant lacked standing to challenge data collection under 50 U.S.C. § 1861, the FISA, and targeted collection program known as PRISM).

[39] MedlinePlus, *What Is DNA?*, *supra* note 34.

bases: "adenine (A), guanine (G), cytosine (C), and thymine (T)."[40] The order and sequence of these bases are known as the genome, with the human genome made up of 3.2 billion bases of DNA.[41] How this code is arranged will dictate "the information available for building and maintaining an organism."[42] DNA can be described as a cookbook that "holds the instructions for making all the proteins in our bodies."[43] The more closely related two individuals are, the greater the percentage of DNA they share.[44]

While DNA sequencing and testing has added to medical knowledge, its importance in criminal law has been transformative.[45] Within criminal law, DNA became a tool used to exonerate the wrongly convicted in 1989.[46] Although DNA evidence has the ability to erase prosecutorial misconduct or right the wrongs of the past, it is dwarfed by law enforcement's use of this technology in investigations.[47] The FBI established the Combined DNA Index System (CODIS) pilot software in 1990 and the DNA Identification Act of 1994 allowed the FBI to establish the DNA Index System for law enforcement purposes.[48] As of August 2021, the FBI's National DNA Index System (NDIS) contained more than 14.7 million offender profiles, 4.4 million arrestee profiles, and 1.1 million forensic profiles, with this information assisting on more than half a million investigations.[49]

State and local law enforcement departments have bucked the trend of using the FBI's CODIS system and have begun to create their own DNA databases, causing a

---

[40] *Id.*

[41] *What Is DNA?*, YOUR GENOME, https://www.yourgenome.org/facts/what-is-dna [https://perma.cc/9VJ7-EUND] [hereinafter Your Genome, *What Is DNA?*].

[42] MedlinePlus, *What Is DNA?*, *supra* note 34.

[43] Your Genome, *What Is DNA?*, *supra* note 41.

[44] *See Autosomal DNA Statistics*, INT'L SOC'Y OF GENETIC GENEALOGY WIKI, https://isogg.org/wiki/Autosomal_DNA_statistics [https://perma.cc/Q56C-NVK5].

[45] *Advancing Justice Through DNA Technology: Using DNA to Solve Crimes*, U.S. DEP'T OF JUST. (Mar. 2003), https://www.justice.gov/archives/ag/advancing-justice-through-dna-technology-using-dna-solve-crimes [https://perma.cc/ZF62-HXPZ] ("DNA technology is increasingly vital to ensuring accuracy and fairness in the criminal justice system.").

[46] *DNA Exonerations in the United States*, THE INNOCENCE PROJECT, https://www.innocenceproject.org/dna-exonerations-in-the-united-states/ [https://perma.cc/X37M-2M5X] (explaining that more than 375 people have been exonerated for crimes by way DNA, with 21 of those people having served time on death row).

[47] Fred Harren, the Bensalem, Pennsylvania Police Department Director describes local DNA databases as "the best thing to come to law enforcement since fingerprints." Jason Kreag, *Going Local: The Fragmentation of Genetic Surveillance*, 95 B.U. L. REV. 1491, 1519 (2015).

[48] *Combined DNA Index System (CODIS)*, FED. BUREAU OF INVESTIGATION, https://www.fbi.gov/services/laboratory/biometric-analysis/codis [https://perma.cc/QG55-WR6A].

[49] *CODIS-NDIS Statistics*, FED. BUREAU OF INVESTIGATION, https://www.fbi.gov/services/laboratory/biometric-analysis/codis/ndis-statistics [https://perma.cc/K5TR-CA9P].

diversification of databases based on jurisdiction.[50] By creating their own databases, state and local authorities are able to skirt federal rules and regulations on the use of the FBI's [51] national database. Local authorities, utilizing their own databases, are also able to benefit from the ability to collect samples from juveniles, victims of crimes, and citizens who respond to calls for voluntary samples to investigate cold cases.[52]

Recently, DTC DNA tests and third-party databases have begun to substantially affect and assist law enforcement. The "Golden State Killer"[53] was believed to have committed over fifty rapes and thirteen murders during the 1970s and 1980s and evaded capture by California authorities.[54] In 2018, investigators obtained "abandoned" DNA samples from the garbage of a man they believed to be the perpetrator.[55] California authorities utilized the consumer DNA testing company GEDmatch to connect abandoned DNA samples from previous crime scenes to a man they believed to be the "Golden State Killer."[56] The man pled guilty and was sentenced to twelve consecutive life terms for a combination of thirteen murders, thirteen kidnappings, and numerous weapons charges.[57]

---

[50] *See* Kreag, *supra* note 47, at 1492 n.1 (noting local DNA databases are employed in "Bensalem, PA; Palm Bay, FL; Hillsborough County Florida Sheriff's Office (Tampa, FL); Lafayette Parish Sheriff's Office (Lafayette, LA); Allegheny County, PA; and the State of Arizona").

[51] *See Frequently Asked Questions on CODIS and NDIS*, FED. BUREAU OF INVESTIGATION, https://www.fbi.gov/services/laboratory/biometric-analysis/codis/codis-and-ndis-fact-sheet [https://perma.cc/U7RG-Y88A] (describing rules and regulations governing an organization's use of the FBI's NDIS system, including not performing familial searches, described as the "intentional or deliberate search of the database conducted after a routine search for the purpose of potentially identifying close biological relatives of the unknown forensic sample associated with the crime scene profile").

[52] Kreag, *supra* note 47, at 1497.

[53] Heather Murphy & Tim Arango, *Joseph DeAngelo Pleads Guilty in Golden State Killer Cases*, N.Y. TIMES (June 29, 2020), https://www.nytimes.com/2020/06/29/us/golden-state-killer-joseph-deangelo.html [https://perma.cc/C6TQ-WRPX].

[54] Erin Hallissy & Charlie Goodyear, *DNA Links '70s 'East Area Rapist' to Serial Killings / Evidence Suggests Suspect Moved to Southern California*, SF GATE (Apr. 4, 2001), http://www.sfgate.com/news/article/DNA-Links-70s-East-Area-Rapist-to-Serial-2935342.php [https://perma.cc/KU8B-6PVF].

[55] Thomas Fuller, *How a Genealogy Site Led to the Front Door of the Golden State Killer Suspect*, N.Y. TIMES (Apr. 26, 2018), https://www.nytimes.com/2018/04/26/us/golden-state-killer.html [https://perma.cc/492B-WJ9R] ("Investigators then obtained what Anne Marie Schubert, the Sacramento district attorney, called 'abandoned' DNA samples from Mr. DeAngelo. 'You leave your DNA in a place that is a public domain,' she said.").

[56] *Id.*

[57] Thomas Fuller, *Golden State Killer Sentenced to Life in Prison Without Parole*, N.Y. TIMES (Aug. 21, 2020), https://www.nytimes.com/2020/08/21/us/golden-state-killer-sentenced.html [https://perma.cc/M465-MYDK] (reporting that the defendant admitted to fifty rapes but could not be charged due to statute of limitations).

GEDmatch is an open-source DNA database that differs significantly from DTC DNA test sites like 23andMe or AncestryDNA. For example, "GEDmatch is a third-party database where you can upload your raw DNA files and be able to use their tools to match with other people regardless of what other company those people tested from."[58] GEDmatch's classic website sports a less modern user interface akin to websites of decades past that only allows visitors the option of registering for an account or logging in with a preexisting account.[59] Sites and services that allow the upload of raw DNA files derived from 23andMe, Ancestry DNA, and MyHeritage are often free and tailored to a host of niches ranging from diet and fitness,[60] to forensic investigations.[61] While terms of service give users the reasonable expectation that their genetic data will only be used in the manner specified, that is not always the case.[62] For example, to help solve a violent assault against a seventy-one-year-old woman, Utah authorities successfully lobbied the head of GEDmatch to relax standards that limited the use of user DNA.[63] Previously, GEDmatch only allowed the use of user DNA to assist law enforcement in homicide or sexual assault cases, reasoning that relaxing standards was appropriate because "police made a compelling case that this [suspect] was a public risk."[64]

It appears this secondary industry for genetic information is ripe for exploitation by law enforcement, as well as by bad actors.

II. NATIONAL SECURITY RISKS OF OPEN-SOURCE DATABASES

The 2019 Department of Defense memo that warned servicemembers about using DTC DNA tests gave no rationale underlying the potential national security concerns in the realm

---

[58] *Getting Started with GEDmatch—A Segment of DNA*, YOUTUBE (Sept. 3, 2019), https://www.youtube.com/watch?v=id7JJ1NoTNk&feature=youtu.be&ab_channel=FamilyHistoryFanatics [https://perma.cc/MVB9-XTVT].

[59] *GEDmatch Login*, GEDMATCH, https://classic.gedmatch.com/login1.php [https://perma.cc/7QZA-BYJA].

[60] Takano, *supra* note 3.

[61] In reference to assisting forensic investigators, certain third-party websites collect genetic data to find suspects and identify victims to help law enforcement solve cold cases. *Frequently Asked Questions*, DNASOLVES, https://dnasolves.com/faq [https://perma.cc/5PLV-ZQ79].

[62] Peter Aldhous, *The Arrest of a Teen on an Assault Charge Has Sparked New Privacy Fears About DNA Sleuthing*, BUZZFEED NEWS (May 14, 2019, 10:15 PM), https://www.buzzfeednews.com/article/peteraldhous/genetic-genealogy-parabon-gedmatch-assault [https://perma.cc/X7XY-34TP].

[63] *Id.*

[64] *Id.*

of mass surveillance.[65] Therefore, it is necessary to assess and discern potential ways that DNA data can be used by adversaries to substantially impact national security.[66] While certain DTC DNA testing companies may secure their data sufficiently, third-party DNA sites that allow for the upload of raw data may be less secure.[67]

A. Vulnerabilities in DTC Sites and DNA Databases

Recently, data breaches, the use of genetic material from DTC services to aid law enforcement, and the national security implications of the laissez-faire approach to handling consumer's information by third-party DNA databases has created an untenable situation. In 2018, MyHeritage, a DNA and genealogy service suffered a hack that disclosed the email addresses and passwords of more than ninety-two million users, with sensitive data like DNA and family tree information being spared.[68] In July 2020, GEDmatch suffered a series of back-to-back hacks that changed user settings, exposing more than a million additional users' data to law enforcement—a setting those GEDmatch users initially opted out of.[69]

To date, 23andMe states that it will seek judicial review if law enforcement requests overly broad information pertaining to national security through an administrative subpoena.[70] Additionally, Ancestry claims they only cooperate with authorities when required by subpoena or other "valid legal process."[71]

---

[65] Shawn Snow, *Pentagon Advises Troops to Not Use Consumer DNA Kits, Citing Security Risks*, MIL. TIMES (Dec. 24, 2019), https://www.militarytimes.com/2019/12/24/pentagon-advises-troops-to-not-use-consumer-dna-kits-citing-security-risks/ [https://perma.cc/S24H-JTTK] ("The Pentagon memo did not provide specific details regarding security risks or how servicemembers could be tracked by using a consumer genetic testing company.").

[66] Antonio Regalado, *The DNA Database Used to Find the Golden State Killer Is a National Security Leak Waiting to Happen*, MIT TECH. REV. (Oct. 30, 2019), https://www.technologyreview.com/2019/10/30/132142/dna-database-gedmatch-golden-state-killer-security-risk-hack/ [https://perma.cc/Z4AM-5MMY].

[67] Peter Ney et al., *Genotype Extraction and False Relative Attacks: Security Risks to Third-Party Genetic Genealogy Services Beyond Identity Inference*, 27 NDSS SYMP. 1, 1–2 (2020), https://dnasec.cs.washington.edu/genetic-genealogy/ney_ndss.pdf [https://perma.cc/W4J9-CLGT].

[68] Alia Wong, *DNA Site's Hack Is Fresh Reminder to Think Twice About Ancestry Testing*, USA TODAY (June 9, 2018, 8:27 AM), https://www.usatoday.com/story/tech/talkingtech/2018/06/08/myheritages-hack-resurfaces-concerns-dna-testing-privacy/675035002/ [https://perma.cc/U8WX-EN5D] (reporting that the genetic data sat on a wholly different server than the private server where user email addresses and passwords were kept).

[69] 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/KX8H-TMHQ].

[70] *23andMe Guide for Law Enforcement*, 23ANDME, https://www.23andme.com/law-enforcement-guide/ [https://perma.cc/C2FA-PXKZ].

[71] *Ancestry Guide for Law Enforcement*, ANCESTRY, https://www.ancestry.com/cs/legal/lawenforcement [https://perma.cc/5ZUR-62MV].

The NSA describes cyberspace threats as the newest and "perhaps the fastest growing" to US economic and national security.[72] DNA databases are third-party services and "allow anyone to upload DNA sequences and search for other users with matching sequences."[73] Some third-party DNA databases store genetic data files (GDFs) from DTC DNA websites as ASCII files.[74] ASCII is a standard coding system initially developed for teletypewriters but became the industry-wide standard for personal computers.[75] Because GDFs are encoded in "simple" ASCII files,[76] open-source databases may not be secure and vulnerable to hacking, and therefore could be a national security risk.[77]

University of Washington researchers sought to show how design choices by third-party services can contribute to security risks.[78] Because the GDFs are coded in industry-standard methods (like ASCII) without any accompanying verification or authentication scheme, researchers concluded that there is nothing stopping adversaries from creating and uploading falsified GDFs that would be indistinguishable from authentic GDFs.[79] Imagine an anonymous email to a prominent political leader that claims to show proof of infidelity through the existence of a fictional child based on falsified DNA data. The email demands either a sum of money or a specific set of demands be met. These types of attacks by adversaries could have major implications not only in politics, but also in corporate espionage, and other areas involving high-profile individuals where damage to one's reputation through blackmailing could be catastrophic.[80] Researchers in the University of Washington experiment found that adversaries can manipulate genetic matches to "spoof" others into believing they have familial relations that do not exist.[81] While this may sound dystopian or

---

[72] *Understanding the Threat*, NAT'L SEC. AGENCY, https://web.archive.org/web/20200410154627/https://www.nsa.gov/what-we-do/understanding-the-threat/ [https://perma.cc/DT62-JKNW] (explaining "[o]ur information networks and technology are constantly at risk from a variety of bad actors using a multitude of techniques").

[73] Andy Fell, *Hobbyist DNA Services May Be Open to Genetic Hacking*, UC DAVIS COLL. OF BIOLOGICAL SCIS. (Oct. 22, 2019), https://biology.ucdavis.edu/news/hobbyist-dna-services-may-be-open-genetic-hacking [https://perma.cc/H595-KQTC].

[74] Ney et al., *supra* note 67, at 2.

[75] *ASCII*, BRITANNICA, https://www.britannica.com/topic/ASCII [https://perma.cc/DY5Q-S5QZ].

[76] Ney et al., *supra* note 67, at 2.

[77] *See* Regalado, *supra* note 66.

[78] Ney et al., *supra* note 67, at 1–2.

[79] *Id.* at 11.

[80] *See* Emily Mullins, *The Era of DNA Database Hacks Is Here*, ONEZERO (July 30, 2020), https://onezero.medium.com/the-era-of-dna-database-hacks-is-here-85a860190622 [https://perma.cc/4EH3-NV9F].

[81] Ney et al., *supra* note 67, at 10.

far-fetched, a group named the Earnest Project may have set events in motion that could lead to the exact scenario contemplated by the researchers in the University of Washington experiment.[82] The group claims to have recovered DNA samples of world leaders like French President Emmanuel Macron, former German Chancellor Angela Merkel, and former President Donald Trump from the 2018 World Economic Forum in Davos, Switzerland and seeks to sell them for up to $65,000.[83]

"Spoofing" in this manner could also disrupt the genetic identity inferences that law enforcement uses to track down familial relationships between recovered genetic information of suspects and existing DNA samples within databases.[84] If those motivated by profit can use spoofing to manufacture familial relationships, they can do the same to misdirect investigators into investigating fake DNA matches.

Alternatively, hacked genetic information could be employed as another factor in larger, open-source intelligence operations. Open-source intelligence is a tool used by allies and adversaries alike to combine innocuous information like a user's web browsing history, geospatial information, and photos to gain insight at a relatively low cost.[85] Combining open-source intelligence with DNA data could be harmful to Americans within the national security apparatus by exposing the genetic identity of American field agents and spies.[86] Because genetic information and DNA can be used to exploit high-value targets in government, corporate, and other areas, deeming DTC DNA testing as a national security threat runs the risk of allowing the national security apparatus to deem all DNA to be relevant, and warrant bulk collection.[87]

---

[82] Emily Mullins, *Trump's DNA Is Reportedly for Sale. Here's What Someone Could Do with It*, ONEZERO (Feb. 14, 2020), https://onezero.medium.com/trumps-dna-is-reportedly-for-sale-here-s-what-someone-could-do-with-it-e4402a9062c2 [https://perma.cc/YFH2-WH4L].

[83] *Id.*

[84] Ney et al., *supra* note 67, at 3, 9.

[85] *INTellingence: Open Source Intelligence*, CENT. INTEL. AGENCY, https://web.archive.org/web/20200303002208/https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/open-source-intelligence.html [https://perma.cc/EE8Y-QQJU].

[86] *See* Regalado, *supra* note 66 ("If a foreign counterintelligence agency grabbed a million American DNA profiles, that country could use genetic genealogy to identify the true identity of American spies or diplomats, locate their relatives, or discover genetic *kompromat* like unacknowledged children. Since other countries don't have such databases for the US to steal, the risk would not be symmetric.").

[87] *See* Kelly Ferrell, *Twenty-First Century Surveillance: DNA "Data-Mining" and the Erosion of the Fourth Amendment*, 51 HOUS. L. REV. 229, 230 (2013) ("Corporations justify 'data-mining' technology as an efficient means of targeting interested consumers, while the government boasts of national security and public safety to rationalize the surveillance technique.").

B. Exploitable DNA Databases

While genetic testing could be a national security threat, inadvertent collection of citizens' data may empower the intelligence community to unwittingly build a massive, searchable genetic database. While this may be unintentional in the United States, it is occurring intentionally in other parts of the world.[88] China is presently using genetic testing and DNA samples to try and map the genetic information of 700 million men to aid in their surveillance capacities.[89] Human rights groups allege that China's government primarily focuses on tracking ethnic minorities.[90] It is estimated that China seeks to collect samples from up to 70 million males, or about 10 percent of its male population.[91] China does not seek to retrieve samples from every male because samples from 5 to 10 percent of their population can reveal familial relations and identify other male relatives.[92]

Recently, the Department of Homeland Security (DHS) sought to modify existing fingerprinting guidance to collect DNA samples from detained migrants and enter those samples into the FBI's CODIS system.[93] The DHS rationalized collection of DNA as a benefit in the event that the "detainee remains in or later reenters the United States and commits such a crime."[94] As of September 2020, the Trump administration, through the DHS, proposed to collect DNA and other "biometric data" of citizens who sponsor prospective immigrants.[95]

Because African Americans and Hispanic Americans are incarcerated at higher rates than white Americans,[96] some argue that preexisting databases like the FBI's CODIS system may suffer from "scope creep."[97] Scope creep occurs when disproportionate

---

[88] Wee, *supra* note 36.

[89] *Id.*

[90] *Id.*

[91] *Id.*

[92] *Id.*

[93] Abigail Hauslohner, *U.S. Immigration Authorities Will Collect DNA from Detained Migrants*, WASH. POST (Mar. 6, 2020), https://www.washingtonpost.com/immigration/us-immigration-authorities-will-collect-dna-from-detained-migrants/2020/03/06/63376696-5fc7-11ea-9055-5fa12981bbbf_story.html [https://perma.cc/W6EJ-K9F6].

[94] DNA-Sample Collection From Immigration Detainees, 85 Fed. Reg. 13,483, 13,488 (Dep't of Just. Apr. 8, 2020) (to be codified at 28 C.F.R. pt. 28).

[95] *Trump Administration Seeks Sweeping DNA Collection of Immigrants, U.S. Sponsors*, REUTERS (Sept. 11, 2020), https://www.reuters.com/article/us-usa-immigration-dna/trump-administration-seeks-sweeping-dna-collection-of-immigrants-u-s-sponsors-idUSKBN26223T [https://perma.cc/4Y4K-G4UN].

[96] *See Criminal Justice Fact Sheet*, NAACP, https://www.naacp.org/criminal-justice-fact-sheet/ [https://perma.cc/UBN7-R4MX].

[97] Thor Benson, *DNA Databases in the U.S. and China Are Tools of Racial Oppression*, IEEE SPECTRUM (June 30, 2020), https://bit.ly/3PyojTJ [https://perma.cc/5UYF-PTZQ].

representation in databases may not be limited to the initial system, and may occur in other unexpected projects or systems in the future.[98] Additionally, the disproportionate scope creep focused on communities of color means that they may be the first and hardest hit in data mining.[99]

III. INTEGRATION OF DNA INTO NATIONAL SECURITY APPARATUS

Because of constitutional protections, different statutory schemes exist to deal with foreign or domestic threats.[100] Genetic data is not limited to a single populace, as people emigrate to different nations around the world.[101] Because of this, it necessarily follows that any genetic information acquired during a foreign-based, national security investigation could have domestic constitutional implications.

A. Domestic Issues

Because of the incredible power DNA holds as an identifier, its widespread availability, and the nature of DNA databases, collection of this data or use in law enforcement investigations implicates concerns for the potential violation of civil liberties.[102] In assessing whether executive authority could theoretically bypass Fourth Amendment concerns in seizing genetic information in the context of national security concerns, *United States v. U.S. District Court* (the *Keith* case) sheds light on how the Supreme Court has ruled previously.[103]

In the *Keith* case, defendants were charged with conspiracy to destroy government property, with one particular defendant charged with the bombing of a CIA office.[104] The defendant sought to have the United States disclose electronic surveillance information to show that the evidence against him was collected unlawfully through warrantless wiretaps.[105] Title III of the Omnibus Crime Control and Safe Streets Act details procedures for the interception and disclosure of wire, oral, and electronic

---

[98] *Id.*

[99] *Id.*

[100] Robert C. Power, *"Intelligence" Searches and Purpose: A Significant Mismatch Between Constitutional Criminal Procedure and the Law of Intelligence-Gathering*, 30 PACE L. REV. 620, 629–30 (2010).

[101] *See* Tom Ulrich, *Historic Migration Patterns Are Written in Americans' DNA*, MIT NEWS (Mar. 5, 2020), https://news.mit.edu/2020/historic-migration-patterns-americans-dna-0305 [https://perma.cc/LY7T-4X7F].

[102] Guest, *supra* note 33, at 1042.

[103] United States v. U.S. Dist. Ct. (*Keith*), 407 U.S. 297, 297–98 (1972).

[104] *Id.* at 299.

[105] *Id.* at 299–300.

communications.[106] At the time of the decision, a relevant portion of the statute stated that "[n]othing contained in this chapter . . . shall limit the constitutional power of the President to take such measures as he deems necessary to protect . . . against actual or potential attack or other hostile acts of a foreign power . . . ."[107] The government contended that electronic surveillance "without prior judicial approval" against the defendant was "a reasonable exercise of the President's power (exercised through the Attorney General) to protect . . . national security."[108] The Court opined that this was not a conferral of additional powers to the president in the realm of electronic surveillance and that the language was "essentially neutral."[109] The Supreme Court held that the government could not conduct warrantless searches based on a domestic national security threat.[110] While this is an instance of communications surveillance, it gives the legal community insight as to how a potential court could interpret a warrantless seizure of genetic data.

For searches conducted for purposes not pertaining to criminal investigations, the "constitutional mandate of reasonableness" governs, where the government interest must be weighed against the "constitutionally protected interests of the private citizen."[111] While the Court has struck down warrantless searches or inspections based on building code violations, it has endorsed the use of a state's police power to enforce minimum standards in preventing damage from natural disasters or to decrease the lethality of epidemics that could devastate densely populated cities.[112] The COVID-19 pandemic continues to affect the United States, and as of March 13, 2022 has claimed the lives of 967,590 Americans.[113] Researchers have recently concluded that "[h]uman genetic factors may contribute to the extremely high transmissibility of SARS-CoV-2 and to the relentlessly progressive disease observed in a small but significant proportion of infected individuals; yet, these factors are largely unknown."[114] In October 2020, "the highest-ranking

---

[106] 18 U.S.C. § 2511.

[107] *Keith*, 407 U.S. at 302 (quoting 18 U.S.C. § 2511(3)).

[108] *Id.* at 301.

[109] *Id.* at 303 ("In short, Congress simply left presidential powers where it found them.").

[110] *Id.* at 321.

[111] Camara v. Mun. Ct. of S.F., 387 U.S. 523, 534–35 (1967).

[112] *Id.*

[113] JOHNS HOPKINS UNIV. & MED.: CORONAVIRUS RES. CTR., https://coronavirus.jhu.edu/ [https://perma.cc/UA7M-KGVV].

[114] Yuan Hou et al., *New Insights Into Genetic Susceptibility of COVID-19: An ACE2 and TMPRSS2 Polymorphism Analysis*, 18 BMC MED. 216, at 2 (July 15, 2020), https://bmcmedicine.biomedcentral.com/track/pdf/10.1186/s12916-020-01673-z.pdf [https://perma.cc/H4AA-2TMB].

officers" of the US "Army, Navy, Air Force, [and] Coast Guard" went into isolation after a Coast Guard admiral contracted COVID-19.[115] The Department of Defense employs 2.91 million servicemembers and civilians.[116] Those serving are connected by familial relations to Americans across the country.[117] Thus, it is not outside the realm of possibility for a national security concern to take the form of a public health issue that affects a segment of the population with specific genetic factors. Identifying this correlation or connection could empower state and federal law enforcement agencies to seize genetic information from DNA databases under the auspices of national security to assist in neutralizing a potential threat.

B. International Issues

Certain cases over the past decade show how courts adjudicate foreign surveillance claims and how the courts tend to favor the government.[118] Article III of the US Constitution limits what cases can be adjudicated in federal court through the doctrine of constitutional standing.[119] To establish Article III standing, "[t]he plaintiff must have suffered or be imminently threatened with a concrete and particularized 'injury in fact' that is fairly traceable to the challenged action of the defendant and likely to be redressed by a favorable judicial decision."[120]

Plaintiffs outside the United States and not a "United States person"[121] may have difficulty establishing standing in court under FISA. Under 50 U.S.C. § 1881(a) of the FISA, the director of national intelligence and attorney general can "acquire foreign intelligence information by jointly authorizing the surveillance of individuals who are not 'United States persons' and are reasonably believed to be located outside the United States."[122]

---

[115] Robin Wright, *The Coronavirus Pandemic Is Now a Threat to National Security*, NEW YORKER (Oct. 7, 2020), https://www.newyorker.com/news/our-columnists/america-the-infected-and-vulnerable [https://perma.cc/U9UC-KFGB].

[116] *About*, U.S. DEP'T OF DEF., https://www.defense.gov/about/ [https://perma.cc/2EZ9-YUR4].

[117] *See supra* Introduction.

[118] *See* Margot E. Kaminski, *Standing After Snowden: Lessons on Privacy Harm from National Security Surveillance Litigation*, 66 DEPAUL L. REV. 413, 415 (2017) ("Courts are almost uniquely disinclined to recognize intangible harms in the area of privacy law.").

[119] Lexmark Int'l, Inc. v. Static Control Components, Inc., 572 U.S. 118, 125 (2014) (quoting Lujan v. Defs. of Wildlife, 504 U.S. 555, 560 (1992)).

[120] *Id.* (quoting *Lujan*, 504 U.S. at 560).

[121] "'United States person' includes citizens of the United States, aliens admitted for permanent residence, and certain associations and corporations." Clapper v. Amnesty Int'l USA, 568 U.S. 398, 401 n.1 (2013) (quoting 50 U.S.C. § 1801(i)).

[122] *Id.* at 401.

Even if one can establish standing under FISA by being a "United States person," they must still establish Article III standing. In *Clapper*, "United States persons" brought suit under the theory that 50 U.S.C. § 1881(a) was unconstitutional.[123] The Supreme Court held that the respondents lacked Article III standing because an injury had not occurred, and their claims of future injury were "too speculative to satisfy the well-established requirement that threatened injury must be 'certainly impending.'"[124]

In *Klayman v. Obama*, plaintiffs brought suit alleging that the government illegally collected "bulk telephony metadata collection under" under the USA Patriot Act of 2001, § 402 of FISA, and the PRISM program under § 702 of FISA."[125] The court ruled that because the telephone metadata collection program under the PATRIOT Act had been discontinued by Congress during the course of litigation and data was only retained for the purposes of litigation, they lacked standing.[126] Appellants' FISA claims were dismissed because the government had "produced uncontroverted evidence that the challenged programs had ceased, which the district court credited. Appellants provide no reason to doubt that finding, let alone enough evidence showing it was clear error."[127] Additionally, appellants challenged the international data collection program known as PRISM.[128] The court applied the essential holding of *Clapper v. Amnesty International* and stated:

> That [a]ppellants cannot rest their alleged injury on bare speculation that their contacts abroad will be targeted simply because they reside 'in geographic areas' that they believe to be 'a special focus' of the U.S. government. Instead, they must allege injury that is 'certainly impending' without relying on a 'highly attenuated chain of possibilities.'[129]

Adjudication in FISA cases highlights how the law enforcement's tactics and national security concerns create information asymmetry that disadvantages potential plaintiffs. Applying these principles to a potential bulk harvesting of DNA data makes this clear. The government launches a widespread program of collecting DNA from targets of their investigation. Family members discover the program. Because the program

---

[123] *Id.*

[124] *Id.* (quoting Whitmore v. Arkansas, 495 U.S. 149, 158 (1990)).

[125] Klayman v. Obama, 759 F. App'x 1, 2 (D.C. Cir. 2019).

[126] *Id.* at 4 ("But if Appellants' injury is only the initial collection of the metadata, as they argue, that injury is not redressable by the relief they seek (expungement). The upshot therefore is the same: Appellants lack standing to pursue the claim.").

[127] *Id.*

[128] *Id.* at 2.

[129] *Id.* at 4 (quoting Clapper v. Amnesty Int'l USA, 568 U.S. 398, 406 (2013)).

thereafter ceased, plaintiffs would not be able to establish standing. Additionally, because of the nature of DNA and how files are anonymized frequently, plaintiffs may struggle with a lack of standing because they will be unable to prove that the anonymized genetic data used by law enforcement belongs to them.[130]

Although FISA deals with obtaining "foreign intelligence information," courts interpret FISA applications, warrants, and claims to explicitly allow evidence collected thereafter to be used for criminal prosecutions.[131] In *United States v. Duggan*, defendants challenged FISA under the theory that it violated the Fourth Amendment's probable cause requirement.[132] The court ruled that the act requires a FISA Judge not to conclude that probable cause exists that the surveillance will lead to the collection of viable information, but simply conclude that there is probable cause that the subject is acting at the direction of a foreign government or organization.[133] The court held that these "less stringent" prerequisites in the issuance of a warrant in a criminal investigation to be a the proper balancing of national security concerns and constitutional rights.[134] Because of this "less stringent standard" in establishing probable cause, and allowing information received in FISA surveillance to be used in domestic criminal investigations, any genetic information recovered could potentially be employed by overzealous investigators, prosecutors, and policy makers. The genetic information could also be used in the pursuit of passive collection and data mining by way of "function creep," where databases created for one purpose will be used for other purposes.[135]

The Second Circuit has interpreted that nothing in the Fourth Amendment or the equal protection clause prevents Congress "from adopting standards and procedures that are more beneficial to United States citizens and resident aliens than to nonresident aliens, so long as the differences are

---

[130] *See* Ney et al., *supra* note 67, at 1–3 (explaining that while recent research has demonstrated that anonymized genetic data can be de-identified, and "identification is easier with more matches[,] . . . [t]he growing size of genetic genealogy databases has challenged assumptions about the inherent anonymity of genetic data because relative matching can be used to re-identify anonymous DNA samples").

[131] United States v. Rosen, 447 F. Supp. 2d 538, 544 (E.D. Va. 2006) (citing 50 U.S.C. § 1801(e)).

[132] United States v. Duggan, 743 F.2d 59, 64–65 (2d Cir. 1984), *superseded by statute on other grounds*, *as recognized in* United States v. Abu-Jihaad, 630 F.3d 102 (2d Cir. 2010). The Fourth Amendment requires that a magistrate find by the totality of the circumstances that "there is a fair probability that contraband or evidence of a crime will be found in a particular place." Illinois v. Gates, 462 U.S. 213, 238 (1983).

[133] *Duggan*, 743 F.2d at 73.

[134] *Id.* at 73.

[135] Ferrell, *supra* note 87, at 251.

reasonable."[136] Genetic information is shared by relatives without regard for citizenship or benefits from constitutional protections.[137] Because of this, function creep could lead to a situation in which an intelligence agency could construe the Second Circuit's understanding of Fourth Amendment and equal protection clause jurisprudence to seize the DNA of nonresident aliens related to resident aliens and US citizens.[138] Thus, an intricately structured investigation could sidestep increased constitutional protections afforded to the class of individuals covered under the FISA.[139]

IV. CONSTITUTIONAL IMPLICATIONS

Because the "wall" between criminal investigations and foreign surveillance has been greatly diminished,[140] it is integral to assess the Fourth Amendment implications of the intelligence community integrating genetic data into investigations.

A. Fourth Amendment Privacy Concerns

Fourth Amendment privacy protections are grounded in *Katz v. United States*' two-pronged test as to whether an individual had a subjective expectation of privacy and whether this expectation is reasonable.[141] In *Maryland v. King*, the Supreme Court held that Maryland's DNA Collection Act requiring arrested individuals to submit to a cheek swab for DNA analysis not to be an unreasonable search under the Fourth Amendment.[142] Within Fourth Amendment jurisprudence, the third-party doctrine emerged, where certain information willingly given to third parties is not assumed to

---

[136] *Duggan*, 743 F.2d. at 75 (citing *Abel v. United States*, *see* 362 U.S. 217 (1960), for Fourth Amendment considerations and *Graham v. Richardson*, *see* 403 U.S. 365 (1971), for equal protection considerations); *id.* at 76.

[137] *See Autosomal DNA Statistics*, *supra* note 44.

[138] *See* Ferrell, *supra* note 87, at 251 (explaining how "[h]ypothetically, an innocent individual could be arrested for a crime that he did not commit and accordingly released, but nonetheless his DNA could remain in the database in order to explore the culpability of the arrestee's family members").

[139] *Id.*

[140] Pearlman & Lee, *supra* note 10, at 722 ("Given the vast resources the government has reportedly dedicated to national security, intelligence, and defense agencies to support data mining and analysis in recent years, the boundaries between citizens' Fourth Amendment rights and government's role in providing for national security have become blurred to a point where citizens are growing concerned over whether such activities have led to an intrusion into civil liberties.").

[141] Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan J., concurring).

[142] Maryland v. King, 569 U.S. 435, 436 (2013) ("The only difference between DNA analysis and fingerprint databases is the unparalleled accuracy DNA provides.").

have a reasonable expectation of privacy.[143] The lack of a reasonable expectation to privacy encompasses telephone pen registers,[144] bank records,[145] and email sender or recipient addresses.[146] With advances in technology, communication, and the advent of social media, there is a concerted effort to rethink the utility of the third-party doctrine as it exists today.[147]

Some legal scholars advocate an approach that balances law enforcement investigative techniques with privacy interests. They distinguish between what "information that citizens knowingly and voluntarily convey to third parties from information that citizens may not know or even suspect they convey to a third party but which is obtained by third parties in their normal course of business."[148] *United States v. Jones*, *Carpenter v. United States*, and the scholarship that flows from these lines of cases illuminate the prospects for Fourth Amendment concerns and DTC DNA testing.[149]

In *United States v. Jones*, the Supreme Court held that the placing of a global positioning system (GPS) tracking device on a car to monitor movements constituted a search and seizure under the Fourth Amendment.[150] Justice Scalia reasoned that the *Katz* formulation on the reasonable expectation of privacy was not the be-all-end-all in analyzing Fourth Amendment violations and that it had "been *added to*, not *substituted for*, the common-law trespassory test" in Fourth Amendment rights.[151] Justice Sotomayor, in her concurrence, argued that the third-party doctrine should be reconsidered, stating that a lack of reasonable expectation to privacy was incompatible with the digital age, where a vast amount of personal information is routinely shared with third parties.[152] Justice Sotomayor cautioned that certain short-term and long-term GPS monitoring necessitated a *Katz* analysis because of the ability to generate "a precise

---

[143] Smith v. Maryland, 442 U.S. 735, 745–46 (1979).

[144] *See id.* (holding that petitioner assumed the risk that the police would obtain phone dialing information).

[145] *See* United States v. Miller, 425 U.S. 435, 435 (1976) (holding that bank records "are not confidential communications but negotiable instruments to be used in commercial transactions").

[146] United States v. Forrester, 512 F.3d 500, 511 (9th Cir. 2008) (analogizing sender and recipient addresses to physical piece of mail's "visible" outside address).

[147] Margaret E. Twomey, Note, *Voluntary Disclosure of Information as a Proposed Standard for the Fourth Amendment's Third-Party Doctrine*, 21 MICH. TELECOMM. & TECH. L. REV. 401, 402 (2015).

[148] *Id.* at 403.

[149] *See* Anthony Barone Kolenc, *"23 and Plea": Limiting Police Use of Genealogy Sites After Carpenter v. United States*, 122 W. VA. L. REV. 53, 56–57 (2019).

[150] United States v. Jones, 565 U.S. 400, 404 (2012).

[151] *Id.* at 407–09.

[152] *Id.* at 417 (Sotomayor, J., concurring).

comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."[153] Justice Sotomayor questioned the utility of the third-party doctrine in the age of modern technology, data generation, and how they relate to the personal information of the user.[154] Justice Sotomayor suggested that the third-party doctrine was inadequate in the internet age and individuals "can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy."[155]

Six years later, in *Carpenter v. United States*, the Court declined to extend the third-party doctrine to cell-site location information (CSLI) because of the uniqueness of those records.[156] In *Carpenter*, the government requested a combination of 154 days of CSLI on the defendant, ultimately obtaining 12,898 location points of the defendant's movements, averaging 101 data points a day.[157] CSLI revealed the location of Carpenter whenever his phone received an incoming call, made an outgoing call, and whenever his phone tapped into a wireless network.[158] With all of the data points, investigators were able to construct maps of his movements.[159] Chief Justice Roberts recognized two guideposts as to what constituted an unreasonable search and seizure when the Constitution was adopted.[160] Chief Justice Roberts elaborated that the Framers' intent in drafting the Fourth Amendment was to secure "the privacies of life" from "arbitrary power"[161] with a related aim "to place obstacles in the way of a too permeating police surveillance."[162] Chief Justice Roberts noted the Court's resistance to allow new surveillance technologies like thermal imaging to "encroach upon areas normally guarded from inquisitive eyes . . . [b]ecause any other conclusion would leave homeowners 'at the mercy of advancing technology.'"[163] Chief Justice Roberts also noted that storage capacities for "modern cells phones created the need for a warrant before searching through its digital contents."[164] These two guideposts—securing the privacy of life against arbitrary

---

153 *Id.* at 415.
154 *Id.*
155 *Id.* at 418.
156 Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).
157 *Id.* at 2212.
158 *Id.* at 2212–14.
159 *Id.* at 2212–13.
160 *Id.* at 2214.
161 *Id.* (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).
162 *Id.* (quoting United States v. Di Re, 332 U.S. 581, 595 (1948)).
163 *Id.* (quoting Kyllo v. United States, 533 U.S. 27, 34–35 (2001)).
164 *Id.* (citing Riley v. California, 573 U.S. 373, 393 (2014)).

power and constructing barriers to unlimited police surveillance—are potential pillars to craft a Fourth Amendment privacy right in a person's genetic information through recognition of the incredible amount of information stored within DNA and its availability to law enforcement.[165]

In his analysis, Chief Justice Roberts discussed the distinction between cases on the "expectation of privacy in" one's physical movements[166] and cases dealing with the Fourth Amendment's third-party doctrine.[167] He further reasoned that because the "deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection, the fact that such information is gathered by a third party does not make it any less deserving of Fourth Amendment protection."[168] In heeding Justice Sotomayor's foresight in *Jones* on the issue of deeply revealing data, Chief Justice Roberts directly quoted her observation on the issue of CSLI revealing a person's "familial, political, professional, religious, and sexual associations."[169] Chief Justice Roberts distinguished the GPS tracking device on a car in *Jones* with the CSLI in *Carpenter* by describing the incredibly close relationship individuals have with their phones and law enforcement obtaining that information as achieving "near perfect surveillance, as if it had attached an ankle monitor to the phone's user."[170] Law professor Anthony Barone Kolenc described the Court's ruling in *Carpenter* as exhibiting a "willingness to expand modern privacy rights while limiting the third party doctrine" and its "far-reaching implications."[171] For Professor Kolenc, a post-*Carpenter* analysis in recognizing a privacy interest for DNA encompasses a five-factor balancing test, including "intimacy, comprehensiveness, expense, retrospectivity, and voluntariness."[172]

With respect to intimacy, activities that are more closely related to deeply personal decisions like religion, politics, sexuality, and movement are "more likely to be protected by the Fourth Amendment."[173] DNA and genetic data invokes those

---

[165] Kolenc, *supra* note 149, at 62.

[166] *Carpenter*, 138 S. Ct. at 2215 (citing United States v. Knotts, 460 U.S. 276 (1983)).

[167] *Id.* at 2216 (citing Smith v. Maryland, 442 U.S. 735, 743–44 (1979)).

[168] *Id.* at 2223.

[169] *Id.* at 2217 (quoting United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)).

[170] *Id.* at 2218.

[171] Kolenc, *supra* note 149, at 61.

[172] *Id.* at 72. Professor Kolenc describes this balancing test as being derived from Justice Kennedy's dissent in *Carpenter*. *Id.* at n.118.

[173] *Id.*

concerns pertaining to personhood, because while it "does not reveal a person's movements, it does reveal the intimate (biological) essence of a person's nature."[174] In assessing how comprehensiveness applies to DNA, "society's expectations about the comprehensiveness of law enforcement's capabilities can influence whether an expectation to privacy is objectively reasonable."[175] Because decoding the human genome and harnessing this power through a cheek swab would have been considered unthinkable decades ago, there may be a privacy interest implicated.[176] The expense factor recognizes the relative ease and inexpensive methods by which law enforcement can obtain data relative to traditional methods of investigation.[177] Scholars look to the case of the Golden State Killer where a serial killer alluded capture for decades but was caught with a simple search of DNA matches in a database.[178] The retrospectivity factor recognizes that law enforcement's ability to glean the details of a criminal subject's past before becoming the target of an investigation weighs "in favor of privacy rights."[179] DNA has the ability to reveal much more than a criminal's past movements.[180] Finally, the fifth factor of voluntariness "recognizes that activities that are less voluntary—either because of societal factors . . . or because of the nature of technology are more likely to be considered private."[181] Here, a user must agree to terms of service to submit any DNA and send in a sample for analysis,[182] but DNA itself is shed through everyday tasks, like eating at a fast food restaurant or getting a haircut.[183]

In applying these five factors of the *Carpenter* decision, Professor Kolenc suggests that a privacy right to DNA may well exist.[184] Even so, when subscribers submit their DNA samples to companies for analysis, they are forming a legal relationship with a third-party entity.[185] The Court in *Carpenter* declined to extend the third-party doctrine to CSLI because of its "unique nature."[186] The Court reasoned that the primary rationales for

---

[174] *Id.* at 72–73.
[175] *Id.* at 73.
[176] *Id.*
[177] *Id.* at 72–73 (quoting Carpenter v. United States, 138 S. Ct. 2206, 2217–18 (2018)).
[178] *Id.* at 73.
[179] *Id.*
[180] *See id.* at 72–73.
[181] *Id.* at 74.
[182] *How It Works*, 23ANDME, https://www.23andme.com/howitworks/ [https://perma.cc/NU5V-YTJ5]; *see Terms of Service*, *supra* note 2.
[183] Kolenc, *supra* note 149, at 74.
[184] *Id.* at 74–75.
[185] *See Terms of Service*, *supra* note 2.
[186] Carpenter v. United States, 138 S. Ct. 2206, 2216–17 (2018).

the third-party doctrine—that only limited information could be gleaned from what is taken and assumption of risk by the individual—did not apply.[187] Further, the Court noted that "seismic shifts in digital technology" mean that CSLI could be incredibly precise because engaging in the modern-day world requires carrying a cell phone.[188] In assessing whether the third-party doctrine applies to DTC DNA companies and third-party databases, it appears that user consent, the ability to manipulate privacy settings, and "deliberate affirmative acts" by users submitting their DNA samples contrast with CSLI, where one only needs to turn on their phone for it to ping a cell tower and provide data to a wireless carrier.[189] Additionally, under the assumption of risk theory, it appears that users understood in various terms of service that "law enforcement could access DNA data with an administrative warrant of the type authorized by the Stored Communications Act, which uses a standard less than Fourth Amendment probable cause."[190]

While these factors suggest that a privacy right might exist in one's own DNA and that the third-party doctrine may not be applied to vitiate a person's privacy interest, that right may be close to worthless because law enforcement can use a relative's DNA to identify the target of an investigation through commonalities in their genetic information.[191] Because no right exists to the genetic information of a biological relative "nothing in [the Fourth] Amendment would prevent police from searching the DNA results of a criminal subject's biological relatives to find an identity match."[192] As of February 2019, more than 26 million people have purchased DTC DNA tests.[193] Scientists recently conducted an experiment where 1.28 million consumer DNA tests were able to theoretically match about 60 percent of Americans with European descent to a third-cousin or closer

---

[187] *Id.*

[188] Kolenc, *supra* note 149, at 72–73 (quoting *Carpenter*, 138 S. Ct. at 2219–20).

[189] *Id.* at 96–99.

[190] *Id.* at 98–99. Under the assumption of risk theory "information knowingly shared with another" will create "reduced expectation of privacy." *Id.* at 88 (quoting *Carpenter*, 138 S. Ct. at 2219).

[191] *See id.* at 76 ("[C]riminal subjects who seek to apply the exclusionary rule to suppress evidence obtained through the search of DNA samples of biological relatives are attempting to vicariously assert the rights of their third-party relatives. The subjects are not the victims. The only ones who could raise an objection would be the biological family members themselves.").

[192] *Id.* at 100.

[193] Antonio Regalado, *More Than 26 Million People Have Taken an At-Home Ancestry Test*, MIT TECH. REV. (Feb. 11, 2019), https://www.technologyreview.com/2019/02/11/103446/more-than-26-million-people-have-taken-an-at-home-ancestry-test/ [https://perma.cc/Y8HH-9FT6] (noting that the companies of Ancestry and 23andMe "now have some of the world's largest collections of human DNA").

match.[194] Because only 5 to 10 percent of a population's DNA is needed to extrapolate the remaining population's DNA,[195] a reasonable expectation of genetic privacy under the Fourth Amendment may no longer be realistic, let alone possible because of the assumption of risk in the digital world.[196] Scholars suggest that it would not be objectively reasonable for society to be willing to accept an asserted privacy right in genetic material of a relative.[197]

B. Constitutional Right to Privacy Concerns

Because a reasonable expectation to privacy in DNA may no longer be possible, it may be necessary to look to other constitutional protections to check overzealous law enforcement investigations. In the realm of national security, the Supreme Court has ruled that Fourth Amendment concerns and values are not the only constitutional rights implicated in adjudication.[198] In *Griswold v. Connecticut*, Justice Douglas described penumbras to provisions of the Bill of Rights, thereby crafting the constitutional right to privacy.[199] This zone of privacy undergirds the guarantee of marriage equality and reproductive rights.[200] Some legal scholars have applied the zone of privacy to genetic information.[201]

This potential argument in favor of a judicially crafted right to privacy for DNA developed from different precedents. In *National Archives and Records Administration v. Favish*, noted that a surviving family member had a valid privacy interest in information surrounding the circumstances of a death.[202] In *Powell v. Schriver*, the Second Circuit held that an incarcerated person has a privacy right as to their HIV status and gender

---

[194] Yaniv Elrich et al., *Identity Inference of Genomic Data Using Long Range Familial Searches*, 362 SCIENCE 690 (2018), https://science.sciencemag.org/content/362/6415/690 [https://perma.cc/J7ES-2B3B].

[195] *See* Wee, *supra* note 36.

[196] Kolenc, *supra* note 149, at 99–100.

[197] *Id.* at 77. "Moreover, such an assertion would be difficult to control with any reasonable limiting principle, since 99.7% of genetic material is also shared with every other person on the planet. In light of that statistic, at what point would such a privacy interest cease?" *Id.*

[198] United States v. U.S. Dist. Ct. (*Keith*)., 407 U.S. 297, 313 ("National security cases, moreover, often reflect a convergence of First and Fourth Amendment values not present in cases of 'ordinary' crime.").

[199] Griswold v. Connecticut, 381 U.S. 479, 484 (1965).

[200] Obergefell v. Hodges, 576 U.S. 644, 665–67 (2015); Roe v. Wade, 410 U.S. 113, 152 (1973).

[201] Guest, *supra* note 33, at 1042.

[202] *Id.* at 1036 (citing Nat'l Archives & Records Admin. v. Favish, 541 U.S. 157, 165–74 (2004)).

identity.[203] While the right to privacy in disclosing one's HIV status was recognized in the Second Circuit previously,[204] the *Schriver* decision moved further towards ensuring a fundamental right to privacy of certain personal medical information, that being HIV status.[205] The basis of the Second Circuit's adoption of these medically centered rights to privacy are the progenies of the Supreme Court's ruling in *Whalen v. Roe*, where the right to privacy extended to "the individual interest in avoiding disclosing personal matters."[206] While the opinion in *Schriver* used dated and potentially offensive terms in describing a transgender person's right to privacy, it nonetheless extended a right to privacy to an additional personal matter, the disclosure of gender identity.[207] While there may be right to privacy in an individual's genetic information under the "personal matters" rationale, this does not dispose of the issue of preexisting DNA in genealogical databases that can identify an individual who is not part of the database.[208] Cases rooted in reproductive rights suggest the Supreme Court would be unwilling to recognize an asserted privacy interest by an individual in another's submission to a genealogical website containing shared DNA, because of the inherent difficulty in crafting "any reasonable limiting principle, since 99.7% of genetic material is also shared with every other person on the planet."[209]

V. LEGISLATIVE ALTERNATIVES

Plaintiffs seeking to challenge the use of their genetic material in any type of investigation will surely have issues in establishing standing.[210] There are also dismal prospects in asserting that this information is constitutionally protected by the Fourth Amendment[211] or the constitutional right to privacy.[212] Because the judiciary is ill-suited to regulate a wayward executive branch at the state or federal level, legislative initiatives are necessary. Amending preexisting

---

[203] *Id.* at 1041 (citing Powell v. Schriver, 175 F.3d 107, 111–13 (2d Cir. 1999)).

[204] Doe v. City of New York, 15 F.3d 264, 267 (2d Cir. 1994) ("Individuals who are infected with the HIV virus clearly possess a constitutional right to privacy regarding their condition.").

[205] *Powell*, 175 F.3d at 112.

[206] Whalen v. Roe, 429 U.S. 589, 599 (1977).

[207] *Powell*, 175 F.3d at 113.

[208] *See* Erlich et al., *supra* note 194.

[209] Kolenc, *supra* note 149, at 77 (citing Planned Parenthood of Se. Pa. v. Casey, 505 U.S. 833, 838 (1992)).

[210] *See* discussion *supra* Section III.B.

[211] *See* discussion *supra* Section IV.A.

[212] *See* discussion *supra* Section IV.B.

federal legislation may not be adequate because of the differences in scope and purpose of relevant laws.[213] This Part discusses those existing federal laws and why amendments to them would be insufficient. This Part then surveys how both state[214] and European[215] lawmakers have created regulations as to consumer data, and how best to craft federal legislation to safeguard genetic data from national security overreach.

A. Existing Federal Legislation

Congress passed the Genetic Information Nondiscrimination Act of 2008[216] (GINA) and the Health Insurance Portability and Accountability Act of 1996[217] (HIPAA) as the significant legislation relating to genetic privacy, procedures for storing information, and remedies. GINA is intended "[t]o prohibit discrimination on the basis of genetic information."[218] Under Title II of GINA, applicants or employees cannot be discriminated against based on genetic information.[219] Employees are protected from being denied health insurance based on genetic information that suggests an increased risk for medical issues like cancer.[220] DNA privacy is not the focus of GINA, and the meaning of "genetic information" has been battled in courts since the laws inception.[221] With some courts looking to the statutory intent of the phrase "genetic information" and others looking to the plain meaning of the same phrase.[222] Part of HIPAA's purpose is to "combat waste,

---

[213] *See* Sonia M. Suter, *GINA at 10 Years: The Battle Over 'Genetic Information' Continues in Court*, 5 J.L. & BIOSCIENCES 495, 496–98 (May 25, 2019).

[214] Sarah Rippy, *US State Comprehensive Privacy Law Comparison*, INT'L ASS'N OF PRIV. PROS. (Sept. 16, 2021), https://iapp.org/resources/article/state-comparison-table/ [https://perma.cc/EUB8-X7UR].

[215] Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and the Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) [hereinafter General Data Protection Regulation].

[216] Genetic Information Nondiscrimination Act of 2008, Pub. L. No. 110-233, 122 Stat. 881 (codified as amended in scattered sections of Titles 26, 29, and 42 of the United States Code).

[217] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of Titles 18, 26, 29 and 42 of the United States Code).

[218] Pub. L. No. 110-233, 122 Stat. at 881.

[219] *Genetic Information Discrimination*, U.S. EQUAL EMP. OPPORTUNITY COMM'N (Sept. 20, 2020), https://www.eeoc.gov/genetic-information-discrimination [https://perma.cc/K2PR-SMUM].

[220] Suter, *supra* note 213.

[221] *Id.* at 499.

[222] *See id.* at 495 ("Over the last ten years, however, the courts have been battling over the meaning of 'genetic information.' One interpretive approach adheres strictly to GINA's statutory language; the second interprets the definition restrictively and contrary to the plain meaning of GINA and its underlying goals.").

fraud, and abuse."[223] Under HIPAA, genetic data cannot be given to schools or employers, but law enforcement agencies can access this information without a warrant "if you're a victim or suspect of a criminal investigation."[224]

Retrofitting or amending GINA or HIPAA to change with technology may have unintended consequences and be inadvisable. In *United States v. Jones*, Justice Alito stated in his concurrence that privacy concerns based on emerging technologies "may spur the enactment of legislation to protect against these intrusions. This is what ultimately happened with respect to wiretapping . . . since that time, the regulation of wiretapping has been governed primarily by statute and not case law."[225] An example of this is the history of Title III of the Omnibus Crime Control and Safe Streets Act of 1968. The Omnibus Crime Control and Safe Streets Act was passed in 1968 to increase the ability of law enforcement to coordinate with the judiciary in the realm of criminal law.[226] Title III established wiretapping oral and wire communications as a means to prevent organized crime.[227] The Electronic Communications Privacy Act of 1986 amended Title III, adding electronic communications to the original scope of written and oral communications.[228] Electronic communications are defined within the statute as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature."[229] The broadening of the scope of the statute to encompass electronic communications without proper regard for the implications of the amending language causes more uncertainty.[230] Some propose amending HIPAA or GINA as a solution to these complex issues.[231] Because DTC DNA testing has become more commonplace in the past decade,[232] folding the issue and all of its complexities into a

---

[223] Pub. L. No. 104-191, 110 Stat. at 1936.

[224] Megan Molteni, *The US Urgently Needs New Genetic Privacy Laws*, WIRED (May 1, 2019, 8:00 AM), https://www.wired.com/story/the-us-urgently-needs-new-genetic-privacy-laws/ [https://perma.cc/EUR5-FTWT].

[225] United States v. Jones, 565 U.S. at 427–28 (Alito, J., concurring).

[226] Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197 (codified as amended in scattered sections of 18 and 34 of the United States Code).

[227] *Id.* § 801, 82 Stat. at 211.

[228] Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, § 101, 100 Stat. 1848, 1848 (codified as amended at 18 U.S.C. § 2510).

[229] 18 U.S.C. § 2510(12).

[230] *See* Melanie B. Harmon, Comment, *Applying Leon: Does the Good Faith Exception Apply to Title III Interceptions?*, 2012 U. CHI. LEGAL F. 323, 330–42 (2012) (discussing a circuit split regarding Title III wiretaps and supposing that "Title III does not explicitly disclaim judicially crafted remedies for interceptions of wire and oral communications, but does so for interceptions of electronic communications").

[231] Hannah Frye et al., *Policy Memo: Genetic Privacy Consumer Protections*, WASH. UNIV. IN ST. LOUIS (Nov. 16, 2020), https://sites.wustl.edu/prosper/policy-memo-genetic-privacy-consumer-protections/ [https://perma.cc/8YNT-MD6Y].

[232] Regalado, *supra* note 193.

statute with its own jurisprudence and precedent like GINA or HIPAA may be inadvisable because any proposed amendment could be misconstrued by courts.

B. European Regulatory Framework and State-Based Data Privacy Initiatives

Because federal genetic privacy legislation is needed to standardize the nation's approach to data security,[233] it is valuable to look at best practices for data privacy. European Union (EU) Regulation 2016/679 is also known as the General Data Protection Regulation (GDPR).[234] Any company that processes personal data of people within EU territory must comply with the law.[235] The EU law "mandates a decentralized, context-specific and risk-based approach to data protection with emphasis on . . . data controllers."[236] Genetic data is deemed "special categories of personal data."[237] Under the GDPR, this type of data is subject to specific technical requirements, like pseudonymization.[238] Pseudonymization, as described by the GDPR, constitutes processing and formatting of data in a manner where it cannot be traced back to the original person without additional identifying information, with this additional information required to be stored separately.[239] Under the GDPR, violations that "go against the very principles of the right to privacy and the right to be forgotten that are at the heart of the GDPR" can "result in a fine of up to €20 million, or 4% of the firm's worldwide annual revenue from the preceding financial year, whichever amount is higher."[240] As of the writing of this note, there have been 1,007 GDPR fines levied totaling more than €1.57 billion in penalties, with the largest single fine handed down to Amazon.com, Inc. at €746 million.[241]

---

[233] Derek Hawkins, *The Cybersecurity 202: Why a Privacy Law Like GDPR Would Be a Tough Sell in the U.S.*, WASH. POST (May 25, 2018), https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/05/25/the-cybersecurity-202-why-a-privacy-law-like-gdpr-would-be-a-tough-sell-in-the-u-s/5b07038b1b326b492dd07e83/ [https://perma.cc/D42F-BNEK].

[234] *FAQ*, GDPR.EU, https://gdpr.eu/faq/ [https://perma.cc/4TWC-PFVB].

[235] *Id.*

[236] Masha Shabani & Luca Marelli, *Re-Identifiability of Genomic Data and the GDPR*, EMBO REPORTS (May 24, 2019), https://www.embopress.org/doi/epdf/10.15252/embr.201948316 [https://perma.cc/3YHF-XQE8].

[237] General Data Protection Regulation, *supra* note 215, art. 9.

[238] *What Are the GDPR Fines?*, GDPR.EU, https://gdpr.eu/fines/ [https://perma.cc/T3LE-QJW5].

[239] General Data Protection Regulation, *supra* note 215, art. 4(5).

[240] *What Are the GDPR Fines?*, *supra* note 238.

[241] *Fine Statistics*, GDPR ENFORCEMENT TRACKER, https://www.enforcementtracker.com/?insights [https://perma.cc/9SSJ-MMJG] (data as of February 2022).

Recently, twenty-seven states have either enacted or are on the road to enacting data privacy legislation.[242] California boasts the nation's largest population at more than 39 million residents, as well as largest economy at more than $3.1 trillion.[243] For these reasons, it is best to focus on California's newly created data protection regime. In November 2020, California's voters passed Proposition 24 also known as the California Privacy Rights Act (CPRA).[244] Some practitioners and academics believe California's CPRA is a means not only to protect Californian's data, but as a means to provide an American jurisdiction to attract European companies to transfer data in compliance with the European GDPR regulations.[245] The CPRA's enforcement structure differs dramatically from the GDPR, with injunctive relief as well as a civil penalty framework that fines violators $2,500 for each violation or $7,500 for each intentional violation.[246] The CPRA vests power in the new created California Privacy Protection Agency to ensure that data of California residents is protected.[247] Other states like Texas passed similar legislation that establishes similar watchdog entities,[248] signaling that legislatures are cognizant of the potential dangers of the exploitation of consumer data.

C. Emerging State-Based Biometric and DTC DNA Privacy Legislation

Recently, states have begun to pass legislation that treats biometric data separately from other types of data that can be stored or transmitted. These laws may give insight into how a federal solution could take shape. In 1998, Illinois, passed the Genetic Information Privacy Act (GIPA).[249] This statute contains

---

[242] Rippy, *supra* note 214.

[243] *Overview of California*, U.S. NEWS & WORLD REP., https://www.usnews.com/news/best-states/california [https://perma.cc/A8HJ-F6HC].

[244] California Privacy Rights Act of 2020, Proposition 24, *in* TEXT OF PROPOSED LAWS, CALIFORNIA GENERAL ELECTION VOTERS INFORMATION GUIDE 42–75 (Nov. 3, 2020) [hereinafter CPRA, Prop. 24], https://vig.cdn.sos.ca.gov/2020/general/pdf/topl.pdf [https://perma.cc/7XS4-SK8A] (approved on Nov. 3, 2020, operative Jan. 1, 2023); *see also* Cynthia Cole et al., *Move Over, CCPA: The California Privacy Rights Act Gets the Spotlight Now*, BLOOMBERG L. (Nov. 16, 2020), https://news.bloomberglaw.com/privacy-and-data-security/move-over-ccpa-the-california-privacy-rights-act-gets-the-spotlight-now [https://perma.cc/PCU4-UNJH].

[245] Natasha G. Kohne et al., *CPRA Rivals GDPR's Privacy Protections and Emphasizes Consumer Choice*, LEXOLOGY (Nov. 11, 2020), https://www.lexology.com/library/detail.aspx?g=f0e4b95c-1f39-44d2-a0f0-81da4fff630f [https://perma.cc/XKU2-BS75].

[246] CPRA, Prop. 24, *supra* note 244, at 74.

[247] *Id.* § 1798.105.

[248] *See* H.B. 4390, 86th Leg., Reg. Sess. (Tex. 2019) (enacted).

[249] Genetic Information Privacy Act, 410 ILL. COMP. STAT. 513/1 (1998).

a private right of action that allows a person to bring suit if their genetic information is misused by a business entity,[250] but the legislative findings and purpose of the law appear to be more of a state analogue to HIPAA.[251] This appeared to be the onset of a state-based initiative to regulate genetic data.[252]

Ten years later, Illinois passed the Biometric Privacy Act (BIPA).[253] BIPA allows for a private right of action entitling plaintiffs to $1,000 in damages per violation or $5,000 in damages per each intentional or reckless violation.[254] Because under BIPA, "biometric identifiers" are confined to "a retina or iris scan, fingerprint, voiceprint, or scan of face geometry," it does not include the type of genetic data stored or controlled by a DTC DNA company.[255] BIPA litigation often takes the form of class action suits, and it has been transformational. In March 2021, the social media giant Facebook settled a class action lawsuit with 1.6 million users for $650 million, in a complaint that alleged that Facebook's "tag suggestions" feature was a violation of BIPA because the technology stored digital scans "of [users'] faces without notice or consent."[256]

In October 2021, California passed their own Genetic Information Privacy Act (California's GIPA).[257] California's GIPA requires [DTC] genetic testing company[ies] to "maintain reasonable security procedures and practices to protect a consumer's genetic data against unauthorized access, destruction, use, modification, or disclosure" and "[d]evelop procedures and practices to enable a consumer to . . . [a]ccess their genetic data."[258] The bill defines DTC "genetic testing companies" as any entity that "[s]ells, markets, interprets, or otherwise offers consumer-initiated genetic testing products or services directly to consumers . . . [a]nalyzes genetic data obtained from a consumer" or "[c]ollects, uses, maintains, or discloses genetic data collected or derived from a direct-to-consumer genetic testing product or

---

[250] *Id.* 513/40.

[251] *Id.* 513/5.

[252] Alexander E. Newkirk, Note, *Someone Else May Own a Piece of You: Lack of Federal Regulation Over Direct-to-Consumer DNA Test Kits*, 20 N.C. J.L. & TECH. 267, 287–96 (2019) (further discussing Alaska's, Maryland's, and New Mexico's privacy laws as they relate to genetic data, yet evading DTC DNA testing companies).

[253] Biometric Information Privacy Act, 740 ILL. COMP. STAT. 14/10 (2008).

[254] *Id.* 14/20.

[255] *Id.* 14/10.

[256] Jennifer Bryant, *Facebook's $650M BIPA Settlement 'A Make-or-Break Moment'*, INT'L ASS'N OF PRIV. PROS. (Mar. 5, 2021), https://iapp.org/news/a/facebooks-650m-bipa-settlement-a-make-or-break-moment/ [https://perma.cc/87BK-77T9].

[257] Lara Compton & Stephnie John, *California's Senate Bill 41: The Genetic Information Privacy Act*, JD SUPRA (Oct. 20, 2021), https://www.jdsupra.com/legalnews/california-s-senate-bill-41-the-genetic-4182899/ [https://perma.cc/8YGE-HRP4].

[258] CAL. CIV. CODE § 56.181(d) (West, Westlaw through ch. 12 of 2022 Reg. Sess.).

service, or is directly provided by a consumer."[259] California's GIPA contains a private right of action, with penalties ranging from $1,000 to $10,000 per violation.[260] Because open-source DNA databases that use unsecure storage methods collect, use, or maintain genetic data from DTC DNA websites,[261] they could potentially fall within the scope of this statute and be subject to suit in California. While a state-based approach may work to tailor a statute to each state's economic uniqueness, the juggernaut of the national security apparatus necessitates a federal response.

D. Potential Federal Solution

While a private right of action may be preferable in giving aggrieved parties the flexibility to bring suit for violations, BIPA class action suits present a cautionary tale, where damages and settlement price tags can be astronomical.[262] The "nationalized" private right of action could be ruinous to DTC DNA companies as well as third-party databases if plaintiffs are able to pursue BIPA class action lawsuits. Using a DTC DNA company like 23andMe to show how these fines would work is instructive. On June 17, 2021, 23andMe Inc., became a publicly traded company, with an initial valuation of $3.5 billion.[263] As of August 13, 2021, the company sported a $770 million cash balance, revenue projections of $250 million for fiscal year 2022, and an "[e]xpanded customer data base of 11.6 million genotyped customers."[264] Even using the smallest fine under California's GIPA at $1,000 per violation, 23andMe could be levied an $11.6 billion fine, more than triple their initial valuation.

Utilizing a GDPR-style fine system reveals potential pitfalls as well. Applying a one-size fits all fine would insulate larger companies, as using the 4 percent gross revenue fine structure of the GDPR would only constitute a paltry €10 million

---

[259] *Id.*

[260] *Id.*

[261] *About GEDmatch*, GEDMATCH, https://www.gedmatch.com/about-us [https://perma.cc/653B-TQNS].

[262] *See* Laura Balson, *Illinois Biometric Act Has Been A Class Action Nightmare, But Things May Get Better*, JD SUPRA (July 19, 2021), https://www.jdsupra.com/legalnews/illinois-biometric-act-has-been-a-class-6205214/ [https://perma.cc/M7D7-VTRP] (detailing other BIPA suits where social media company TikTok settled a claim based on facial recognition technology for $92 million, Wal-Mart settled a claim dealing with employee palm scanners for $10 million).

[263] Kristen V. Brown, *23andMe DNA-Testing Firm Goes Public Following Branson Deal*, BLOOMBERG (June 17, 2021), https://www.bloomberg.com/news/articles/2021-06-17/23andme-dna-testing-company-goes-public-following-branson-deal [https://perma.cc/NEV7-86FF].

[264] *23andMe Reports FY2022 First Quarter Financial Results*, 23ANDME (Aug. 13, 2021), https://investors.23andme.com/news-releases/news-release-details/23andme-reports-fy2022-first-quarter-financial-results [https://perma.cc/X5LM-SBJG].

fine for 23andMe.[265] Because potential damages faced by defendant's who violate a federal solution would be cataclysmic and have a chilling effect,[266] it may be more prudent to impose GDPR-style fine caps at significantly higher percentages.

Without a private right of action, it would fall to government regulators to enforce this proposed legislation. Within the federal government, no administrative agency exists for data privacy, but the Federal Trade Commission (FTC) is the rough equivalent of a regulatory authority of this type.[267] In the original FTC Act of 1914, the newly formed agency was only empowered by Congress "to prevent persons, partnerships, or corporations, except banks, and common carriers subject to the Acts to regulate commerce, from using unfair methods of competition in commerce."[268] Today, the FTC describes itself as having a twofold mission of "protect[ing] consumers and promot[ing] competition."[269] In 2019, the FTC held hearings over the course of two days on their approach to consumer privacy.[270] During the hearings, FTC Commissioner Noah Joshua Phillips acknowledged that while advocates had been studying consumer data privacy for years, the issue has "come out of nowhere" to lawmakers and policymakers.[271] The FTC has also failed to enforce its own orders against companies like Google or impose fines against companies like Uber.[272] Because of the failure of federal lawmakers to pass legislation resembling the European GDPR, some have argued that a data protection agency should be created.[273]

With many states drafting protections for consumer data,[274] and most other advanced economies creating agencies to do the

---

[265] *What Are the GDPR Fines?*, *supra* note 238.

[266] Balson, *supra* note 262 ("For large companies, the alleged damages can be in the millions or billions of dollars, even without a single injured plaintiff in the class. For small companies, a BIPA lawsuit can mean the end of the business. And for defense attorneys, there have been very few strategies for effectively defending a client caught unaware of the statutory requirements.").

[267] Hawkins, *supra* note 233.

[268] Federal Trade Commission Act, Pub. L. No. 63-203, 38 Stat. 717, 719 (1914) (codified as amended at 15 U.S.C. §§ 41–58).

[269] *Mission*, FED. TRADE COMM'N, https://www.ftc.gov/about-ftc/what-we-do [https://perma.cc/DUP3-NXUP].

[270] *Hearings on Competition and Consumer Protection in the 21st Century*, FED. TRADE COMM'N (Apr. 9-10, 2019), https://www.ftc.gov/news-events/events-calendar/ftc-hearing-competition-consumer-protection-21st-century-february-2019 [https://perma.cc/8GSD-SAH6].

[271] FED. TRADE COMM'N, PREPARED REMARKS OF COMMISSIONER NOAH JOSHUA PHILLIPS, FTC HEARING #12: THE FTC'S APPROACH TO CONSUMER PRIVACY (Apr. 9, 2019).

[272] *The U.S. Urgently Needs a Data Protection Agency*, ELEC. PRIV. INFO. CTR., https://epic.org/dpa/ [https://perma.cc/NXU8-U9GV].

[273] *Id.*

[274] Cynthia Brumfield, *12 New State Privacy and Security Laws Explained: Is Your Business Ready?*, CSO (Dec. 28, 2020), https://www.csoonline.com/article/3429608/11-new-state-privacy-and-security-laws-explained-is-your-business-ready.html?page=2 [https://perma.cc/WR37-8KLF].

same, any federal legislation should create a new agency as well. Accountability, by regulatory oversight on standards for DNA data storage should be crafted to ensure that those handling consumers' DNA secure it, lest genetic material becomes a national security risk and opens the door for law enforcement agencies to gain access to the data for a domestic or foreign based investigation.[275]

While there are many scientific and technical issues with drafting federal legislation, a major issue that must be assessed is whether statutory language should be ambiguous to allow for judicial discretion or whether it would be more effective to employ muscular regulations. In attempting to craft a federal solution, legislators can either create minimum standards for security, or utilize vague language that courts will then construe. In the realm of minimum standards, Massachusetts remains an outlier in creating minimum standards for storing personal information.[276] Their approach generates regulations with minimum standards for things like secure user authentication protocols, secure access control measures, encryption requirements, and training and education on these matters.[277] Because DNA files are uploaded to some third-party databases in formats that are similar to many other types of files, they can be easily falsified.[278] Researchers have commented that a few different design choices can negate this issue. One includes limiting DNA data that can be entered into a database to what has been previously generated by a DTC DNA company.[279] Another approach would be to limit searches of genetic samples with a "minimum degree of relatedness," because "[t]his will restrict the possible set of GDFs an adversary can target but does not significantly affect usability because unrelated GDFs are rarely compared."[280] Although this may be a significant issue in thrusting compliance on businesses, there is evidence of a secondary market for small businesses seeking to comply with European and state-specific data privacy laws, where they provide privacy consulting.[281] Thus, a secondary industry

---

[275] Vladeck, *supra* note 28, at 336 ("Put another way, if the government is not allowed to access the bulk telephone records it has collected under section 215 of the USA PATRIOT Act until it has 'reasonable articulable suspicion' that a specific phone number is directly relevant to an ongoing terrorism investigation, should there be additional legal constraints in place to govern what happens once it *has* validly accessed that data, both initially and downstream?").

[276] 201 MASS. CODE REGS. 17.04 (2021).

[277] *Id.*

[278] Ney et al., *supra* note 67, at 2 (explaining that genetic data files from direct-to-consumer DNA websites are saved as ASCII files).

[279] *Id.*

[280] *Id.* at 11.

[281] Osano is one such business which provides consulting for compliance with GDPR and state specific privacy laws. *See The World's Most Trusted Data Privacy Software Platform | Osano*, OSANO, https://www.osano.com/ [https://perma.cc/A3UM-8JWA].

could be created for DTC DNA companies and DNA databases to consult with. Applying the approach of the GDPR's pseudonymization to minimum standards in conjunction with protective authentication factors could be a potent bulwark in securing DNA, whether it be DTC DNA testing sites or third-party DNA databases.

Alternatively, utilization of a "reasonable security measures" standard like California's GIPA for violations[282] may go the way of Illinois' BIPA, where the reasonableness standard leaves companies to ponder how it will be applied by courts.[283] This would signal to DTC DNA companies and third-party DNA databases that they must not only secure the data in a reasonable manner, but continue to develop "reasonable security procedures," as a court can calibrate the standard in fact-specific inquiries during any given lawsuit. This may work well as the Supreme Court has been receptive to changing jurisprudence with technology.[284] That said, DNA is too valuable to wrong even once, because there is only so much DNA that can be collected before every person can be tracked.[285] Time is of the essence and Congress must be cognizant of the effects of any proposed legislation. A heightened GDPR-style fine structure, coupled with a limited private right of action and a "reasonable security procedures" judicial standard of review, would give courts the flexibility to grant consumer's recompense for injuries, incentivize DTC DNA companies and third-party databases to adopt security measures, and grant judicial discretion to allow for changes in technology and circumstances.

CONCLUSION

In his concurrence in *United States v. Jones*, Justice Alito stated that "[d]ramatic technological change may lead to periods in which popular expectations are in flux and may ultimately produce significant changes in popular attitudes" and "[n]ew technology may provide increased convenience or security at the

---

[282] CAL. CIV. CODE § 56.181(d) (West, Westlaw through ch. 12 of 2022 Reg. Sess.).

[283] David J. Oberly, *Satisfying BIPA's Reasonable Security Requirement*, BLOOMBERG L., https://www.blankrome.com/sites/default/files/2021-06/satisfying_bipas_reasonable_security_requirement.pdf [https://perma.cc/4H6C-V9V3] (explaining that because Illinois' BIPA does not hold businesses to strict liability for violations and the structure of the law, litigants must "establish that any data breach event resulted from the company's failure to implement and maintain reasonable security practices").

[284] Carpenter v. United States, 138 S. Ct. 2206, 2222 (2018) ("When confronting new concerns wrought by digital technology, this Court has been careful not to uncritically extend existing precedents.").

[285] *See* Elrich et al., *supra* note 194.

expense of privacy, and many people may find the tradeoff worthwhile."[286] At this critical juncture, it may be that the prevalence of DTC DNA tests and third-party databases have erased any reasonable expectation of privacy in one's genetic information and biological essence.[287] As genetic information becomes less of a personal or private matter, the likelihood this data being exploited by adversaries increases.[288] In addition, the fox is guarding the chicken coop, where the present state of affairs allows law enforcement to use this data in investigations without a person's knowledge or consent,[289] and can be harnessed by the national security apparatus to increase their surveillance capacities. Without effective legislation to reinforce genetic privacy, the judiciary will be the lone sentry on the "wall" between foreign and domestic intelligence and law enforcement operations, and it is ill-equipped to do so. Thus, the potential costs to civil liberties in treating genetic data as a national security threat is outweighed by the potential misuse and exploitation by the national security apparatus. If given an inch in the intelligence sphere, the national security apparatus will take a mile. DTC DNA tests should not be seen as a national security threat, because then a cheek swab becomes a shortcut to mapping America's genome.

Elias Rios III[†]

---

[286] United States v. Jones, 565 U.S. 400, 427 (2012) (Alito, J., concurring).

[287] Kolenc, *supra* note 149, at 153.

[288] *See* Ney et al., *supra* note 67, at 3–11.

[289] Lindsay Van Ness, *DNA Databases Are Boon to Police But Menace to Privacy, Critics Say*, PEW CHARITABLE TRS. (Feb. 20, 2020), https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2020/02/20/dna=databases-are-boon-to-police-but-menace-tp-privacy-critics-say [https://perma.cc/TAD3-25RK].

[†] J.D. Candidate, Brooklyn Law School, 2022; M.A. University of Oklahoma, 2016; B.A. Alfred University, 2011. I would like to thank the entire *Brooklyn Law Review* staff, especially Ben See, Crystal Cummings, and Kellie Van Beck for helping me get this note across the finish line. Special thanks to my wife, Emily, for her patience, support, and kindness; my dad, Elias Rios Jr., for inspiring me to always challenge myself; and all my mentors while I served in the United States Air Force. I dedicate this note to the memory of Cathy Rios.