HOMELAND ADVANCED RECOGNITION TECHNOLOGY (HART) DATA COLLECTION: FOURTH AMENDMENT CONSIDERATIONS & SUGGESTED STATUTORY ALTERNATIVES

BRANDON R. THOMPSON

"Big Brother Is Watching You." – George Orwell, 1984[1]

I. INTRODUCTION

"Who watches the Watchmen?"[2] In the realm of biometric data privacy, the answer remains ominously opaque. The government craves biometric data for law enforcement purposes[3] and the private sector sees boundless opportunity in targeted marketing.[4] Their objective? You. But who may be targeted, what data may be collected, and where? Even more fundamental, why is biometric data privacy essential even when balanced against national security concerns?

There is no single definition for the term "biometric data."[5] However, the National Institute of Standards and Technology defines "biometrics" as an "[a]utomated recognition of individuals based on their biological and behavioral characteristics"[6] that consists of "unique personal attributes."[7] In short, it is "something you are."[8] Biometric data—and its collection—also raises another timely question for the age of smart phones and location data-

---

[1] GEORGE ORWELL, 1984 1 (1949).

[2] JUVENAL, THE SATIRES OF JUVENAL: SATIRE VI (G.G. Ramsay trans., 1918). Juvenal's Latin phrase "*Quis custodiet ipsos custodes?*" may be translated in English as "Who will ward the warders?" The phrase has grown popular in recent years, notably appearing in noire superhero films such as *The Watchmen* and *Batman v. Superman: Dawn of Justice* where it is employed to highlight the futility of ordinary citizens against their supposed guardians. *See* BATMAN V. SUPERMAN: DAWN OF JUSTICE (Warner Bros. 2016), THE WATCHMEN (Warner Bros. 2009).

[3] *See, e.g.*, *Fingerprints and Other Biometrics*, FED. BUREAU OF INVESTIGATION, https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics (last visited Sept. 30, 2019).

[4] *E.g.*, Freddy Aurso, *Biometric Data—Will Future Marketers be able to Target Your Emotions?*, SOCIALMEDIATODAY (Nov. 5, 2016), https://www.socialmediatoday.com/technology-data/biometric-data-will-future-marketers-be-able-target-your-emotions.

[5] *See* John D. Woodward, *Biometric Scanning, Law & Policy: Identifying the Concerns—Drafting the Biometric Blueprint*, 59 U. PITT. L. REV. 97, 99 (1997) (broadly defining biometrics as "the automated technique of measuring a physical characteristic or personal trait of an individual and comparing that characteristic or trait to a database for purposes of recognizing that individual"). *See generally* Rivera v. Google, Inc., 238 F. Supp. 3d 1088 (N.D. Ill. 2017) (arguing over what data constitutes a "biometric identifier" under Illinois law), PAUL A. GRASSI ET AL., U.S. DEP'T OF COMM., NAT'L INST. OF STANDARDS & TECH., DIGITAL IDENTITY GUIDELINES (2017), https://doi.org/10.6028/NIST.SP.800-63-3.

[6] GRASSI ET AL., *supra* note 6, at 43.

[7] *Id*. at 13.

[8] *Id*. at 12.

tracking apps,[9] namely, what control do you have over the very essence that makes you, you?

Since September 11, 2001, federal agencies have systematically broadened the scope of their biometric data collection mechanisms to meet ever-increasing demand for comprehensive border security and national security initiatives.[10] Unlike a driver's license, passport, or even Social Security card, unique biometric datum, such as an individual's fingerprint or retinal scan, is an immutable identity signifier[11] that "cannot be replaced or modified if compromised."[12] For the federal government, the allure of biometric data's immutability is its perceived reliability and fraud resistance.[13] Post-9/11, agencies must sift through mounds of data efficiently to find the proverbial needle in the haystack before an attack occurs, all while balancing Americans' privacy rights.[14] For this reason, biometric data collection is seen by many as the "gold standard" for efficient identification, screening, and identity management systems.[15]

However, while the capacity for federal agencies to collect millions of immutable identifiers has grown exponentially in the past few decades, the law remains mired in antiquity.[16] In fact, there are currently no federal laws that directly police the use of facial recognition technology in the national security context.[17] Unlike the targeted, individualized collection of convicted criminals' biometric data, the Department of Homeland Security (DHS) and other agencies have moved toward broad collection of even suspicionless individuals' immutable data.[18]

The broad DHS collection this paper will address raises questions of both the scale and form of data collection. On scale, for example, DHS seeks to gather vast amounts of biometric data from citizens and non-citizens alike

---

[9] *Compare* Simon Chandler, *We're Giving Away More Personal Data Than Ever, Despite Growing Risks*, VENTUREBEAT (Feb. 24, 2019, 8:35 AM), https://venturebeat.com/2019/02/24/were-giving-away-more-personal-data-than-ever-despite-growing-risks/ (discussing the myriad of studies that show Americans are willing to share personal data with companies despite recent data-related scandals and breaches), *with IT Pros Still Don't Trust Biometrics*, BIOMETRIC TECH. TODAY 1, 1–2 (2018).

[10] Laura K. Donohue, *Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age*, 97 MINN. L. REV. 407, 416 (2012).

[11] *See* Margaret Hu, *Biometric ID Cybersurveillance*, 88 IND. L.J. 1475, 1477–78 (2013) [hereinafter Hu, *Biometric ID*]; *see also* Erin Jane Illman, *Data Privacy Laws Targeting Biometric and Geolocation Technologies*, 73 BUS. L. 191, 195 (2017) (including facial geometry and fingerprints as examples of biometric data).

[12] Illman, *supra* note 11, at 195.

[13] Hu, *Biometric ID*, *supra* note 11, at 1477–78.

[14] The Department of Homeland Security, for example, currently uses the Automated Biometric Identification System (IDENT) to process over 300,000 biometric "transactions" per day, consolidating a database of over 220,000,000 biometric transactions on 160,000,000 unique persons. *See* WILLIAM GRAVES, DEP'T OF HOMELAND SEC., US VISIT: THE WORLD'S LARGEST BIOMETRIC APPLICATION 4 (2010), *Biometrics*, DEP'T OF HOMELAND SEC. (Feb. 6, 2017), https://www.dhs.gov/biometrics [hereinafter *Biometrics*].

[15] Hu, *Biometric ID*, *supra* note 11, at 1537.

[16] Donohue, *supra* note 10, at 414.

[17] *Id*. at 414–15.

[18] *Compare* United States v. Kincade, 379 F.3d 813 (2004) (discussing whether the Fourth Amendment permitted compulsory DNA profiling, and concluding that the balancing test between individual privacy interests versus the public's interest in identifying repeat criminal offenders favored the public/State), *with* U.S. GOV'T ACCOUNTABILITY OFFICE, HOMELAND SECURITY ACQUISITIONS: LEVERAGING PROGRAMS' RESULTS COULD FURTHER DHS'S PROGRESS TO IMPROVE PORTFOLIO MANAGEMENT 43 (2018) (discussing Customs and Border Protection's goal to obtain personally identifying biometric data for every passenger entering and exiting the U.S.) [hereinafter GOV'T ACCOUNTABILITY OFFICE REPORT].

both at the border (*e.g.*, persons traveling into and out of the U.S. and immigrants applying for a visa) and beyond (*e.g.*, those applying for TSA "Pre-Check" and parents adopting children from abroad).[19] Some of this collection may be voluntary, but some measures, such as requiring fingerprints at the border from asylum seekers, are necessarily coercive (even if they are sound policy). Lastly, DHS has not stated how some identifiers, such as voice data, will be collected and whether they will be obtained voluntarily or not.

Form is an issue as well, since DHS intends to gather this data via "formal or informal information sharing agreements or arrangements" from "other federal agencies, foreign partners, and state and local partners."[20] Collection through informal arrangements with foreign partners and local officials will likely result in haphazard and decentralized collection and insufficient standardization,[21] plausibly infringing upon U.S. citizens' Fourth Amendment rights.

Thus, through scale and form, emerging biometric collection systems, like DHS's Homeland Advanced Recognition Technology (HART) system,[22] allow the government to "ascertain the identity (1) of multiple people; (2) at a distance; (3) in public space; (4) absent notice and consent; and (5) in a continuous and on-going manner."[23]

The federal government has long touted broad-based biometric data collection as inherently "privacy enhancing" due to the data's efficiency and immutability, which should, in theory, limit false positives and other identification errors.[24] On the other hand, many privacy rights advocates counter that collection of data from suspicionless persons uses biometric data "in a privacy-threatening . . . way."[25] This is particularly relevant as the government moves to expand data-sharing capabilities between agencies.[26] In this way, the September 11 attacks ushered upon the United States an unprecedented period of "collaborative enforcement" in both the national security and immigration spheres.[27]

Traditionally, the Fourth Amendment's prohibition on unreasonable searches and seizures[28] has been used to curb federal searches of citizens'

---

[19] Symposium: *The Second Wave of Global Privacy Protection: Immigration Policing and Federalism Through the Lens of Technology, Surveillance, and Privacy*, 74 OHIO ST. L.J. 1105, 1127 (2013) [hereinafter *The Second Wave*].

[20] PHILIP S. KAPLAN, NAT'L IMMIG. LAW CTR., COMMENTS ON NOTICE OF A NEW SYSTEM OF RECORDS: DEPARTMENT OF HOMELAND SECURITY/ALL-041 EXTERNAL BIOMETRIC RECORDS (EBR) SYSTEM OF RECORDS 2 (2018), https://www.nilc.org/wp-content/uploads/2018/08/NILC-NIPNLG-Comments-EBR-2018-05-23.pdf. *See generally* Privacy Act of 1974, 5 U.S.C. § 552a (1974), System of Records, 83 Fed. Reg. 17829 (Apr. 24, 2018).

[21] SCOTT ELLISON ET AL., NEPTUNE, FEDERAL BIOMETRICS: DISJOINTED PROGRESS 2 (July 2016), http://www.blackarchpartners.com/media/58674/biometrics.pdf ("Historically, DHS biometric programs have been stymied by the lack of clear policy guidelines and poor organizational structures.").

[22] *See infra* notes 40–46.

[23] Donohue, *supra* note 10, at 415.

[24] Bert-Jaap Koops & Ronald Leenes, *'Code' and the Slow Erosion of Privacy*, 12 MICH. TELECOMM. & TECH. L. REV. 115, 166 (2005).

[25] *Id.*

[26] ELLISON ET AL., *supra* note 21, at 2.

[27] See, for example, the collaborative counterterrorism efforts between the DHS, DOJ, and local law enforcement agencies. *See, e.g.*, Trevor George Gardner, *Immigrant Sanctuary as the "Old Normal": A Brief History of Police Federalism*, 119 COLUM. L. REV. 1, 62–63 (2019).

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

personal effects.[29] However, the Fourth Amendment's utility has not carried over into the national security context[30] where biometric data collection is at issue. Because of this, it may fall on Congress to pass legislation delineating the scope of biometrics collection.

Part II of this paper will provide background for DHS's implementation of the HART data collection system. Next, Part III will include the bases for biometric data collection, followed in Part IV by a consideration of the potential pitfalls endemic to the integration of biometric data with biographic data. Part V will consist of a Fourth Amendment analysis of the HART system's biometric collection. Finally, the paper will conclude with recommendations for how Congress may regulate biometric data collection systems while preserving national security interests.

Through the analysis discussed above, this paper will contend first, that the Fourth Amendment should serve as a check on suspicionless collection of advanced biometric data through a limited private right of action and, second, that Congress should pass new legislation delineating the scope, use, and destruction of biometric data collection of U.S. persons to mitigate this otherwise unfettered surveillance state.

II. BACKGROUND

A. IDENT & EARLY BIOMETRIC DATA COLLECTION

Since the 1990s, a number of federal administrative agencies have utilized biometric data collection in a limited set of immigration-related contexts. In 1994, DHS established the Automated Biometric Identity System (IDENT) to collect biometric data (mainly fingerprints) to streamline immigration and border enforcement.[31] Even with this narrow purpose, IDENT existed as one of only a handful of biometric data collection systems.[32]

However, "IDENT has evolved over the years into the central DHS-wide system for the storage and processing of biometric data."[33] The September 11 attacks dramatically expanded IDENT's mandate to include biometric data collection at any border or port of entry, whether entering or exiting the country, for both non-citizens and citizens alike.[34] Between 2001 and 2014, DHS relied on IDENT to collect the fingerprints of a variety of persons who constituted a national security interest, including:

> [S]ubjects who have had any contact with DHS, other agencies, and even other governments including visa applicants at U.S. embassies and consulates, noncitizens traveling to and from the United States,

---

[29] *See* Riley v. California, 573 U.S. 373, 381–84 (2014).

[30] Carpenter v. United States, 138 S. Ct. 2206, 2210 (2018) (deciding "not [to] consider other collection techniques involving foreign affairs or national security").

[31] U.S. DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR THE AUTOMATED BIOMETRIC IDENTIFICATION SYSTEM (IDENT) 2 (Dec. 7, 2012) [hereinafter IDENT PRIVACY IMPACT ASSESSMENT].

[32] Donohue, *supra* note 10, at 420.

[33] *Id*.

[34] Anil Kalhan, *Immigration Surveillance*, 74 MD. L. REV. 1, 29–31 (2014); *see* GOV'T ACCOUNTABILITY OFFICE REPORT, *supra* note 18, at 43 (discussing the implementation of an "Entry-Exit" biometric data collection program as the technology becomes feasible).

> noncitizens applying for immigration benefits (including asylum), unauthorized migrants apprehended at the border or at sea, suspected immigration law violators encountered or arrested within the United States, and even U.S. citizens approved to participate in DHS's "trusted traveler" programs or who have adopted children from abroad. Given its data collection and retention practices, IDENT contains fingerprint records for many naturalized U.S. citizens who were fingerprinted before naturalizing and lawfully present noncitizens . . . .[35]

Each time that an individual's biometric identifier is uploaded to the IDENT database by a collector—Immigration and Customs Enforcement (ICE), Customs Border Patrol (CBP), Citizenship and Immigration Services (CIS), the Department of State, and others—the system logs the data transfer as an "encounter."[36] A far cry from its initial mandate for simple fingerprint collection, today, IDENT stores, processes, and shares digital fingerprints, photographs, iris scans, and facial images.[37] DHS and other national security agencies then link this biometric data with biographic information to construct detailed and holistic portraits of U.S. persons.[38] To date, IDENT has logged biometric data on 160 million unique identities through over 220 million encounters.[39] Through IDENT and other data collection systems, "DHS manages over 10 billion biographic records,"[40] though the exact number of individual biometric data points stored in IDENT is unpublished.

Now, a quarter-century after IDENT's initial implementation, DHS is moving to phase the system out.[41] The government's shift away from IDENT signals federal agencies' insatiable desire for more data.[42] In fact, the IDENT system has become inoperable principally because its processing capabilities—300,000 daily encounters—no longer meets the agency's surging need to gather more and more biometric data.[43] In IDENT's place,

---

[35] *The Second Wave*, *supra* note 19, at 1127.

[36] IDENT PRIVACY IMPACT ASSESSMENT, *supra* note 31, at 2.

[37] PRIVACY IMPACT ASSESSMENT FOR THE AUTOMATED BIOMETRIC IDENTIFICATION SYSTEM (IDENT), DEP'T OF HOMELAND SEC., DHS/NPPD/PIA-002 2 (Dec. 7, 2012), https://www.dhs.gov/sites/default/files/publications/privacy-pia-nppd-ident-december2012.pdf.

[38] ELLISON ET AL., *supra* note 21, at 3–4. The Department of Defense, for example, has enacted a "shift away from the current biometrics and forensics capability-centric focus to a more holistic concept of identity—biometric, biographical, and contextual attributes that help distinguish a friend from an adversary. However, DOD admits that it has yet to define the concept of identity . . . ." *Id*. DHS Privacy Impact Assessments have also stated that biometric data is linked with biographic data. IDENT PRIVACY IMPACT ASSESSMENT, *supra* note 31, at 6 (stating that IDENT records contain both biometric and biographic data, even records of past and present whereabouts).

[39] WILLIAM GRAVES, DEP'T OF HOMELAND SEC., US VISIT: THE WORLD'S LARGEST BIOMETRIC APPLICATION 4 (2010).

[40] DHS IMMIGRATION DATA INTEGRATION INITIATIVE, DEP'T OF HOMELAND SEC. 13 (Sept. 14, 2017) (Conf. Rep.), https://www.eff.org/document/dhs-immigration-data-integration-initiative-slide-presentation.

[41] 2018 PRIVACY OFFICE ANN. REP., DEP'T OF HOMELAND SEC., 36, 57 (2018), https://www.dhs.gov/sites/default/files/publications/dhs%20privacy%20office%202018%20annual%20report%20FINAL%2010-10-2018.pdf.

[42] ELECTRONIC PRIVACY INFORMATION CENTER, FOIA REQUEST: HART PRIVACY IMPACT ASSESSMENT 1–2 (2018) [hereinafter FOIA REQUEST].

[43] *Id*.

DHS is slowly rolling out a new data collection system to replace the old: the Homeland Advanced Recognition Technology (HART).[44]

B. DHS HART'S EXPANSION OF BIOMETRIC DATA COLLECTION

DHS began implementing HART in 2018 with plans to improve IDENT in three significant ways.[45] First, the system's capabilities for collecting and storing biometric data would be vastly expanded.[46] Second, the types of data collected would be increased and diversified by including new identifiers like voice data, scars and tattoos, and other physical characteristics.[47] Finally, the system's potential for sharing information with other non-DHS entities (both foreign and domestic) would be augmented and streamlined.[48] According to the Office of Biometric Information Management (OBIM) within DHS, HART is a necessary successor to IDENT because of "escalating demands for biometric analysis" external to the agency.[49] In sum, HART is intended to perform as a "modular system . . . includ[ing] greater efficiencies, lower costs of operations, increased data volumes, and the capability of incorporating multiple and new biometric modalities."[50]

In practice, DHS has designed HART's collection capabilities to far surpass anything attainable through IDENT.[51] HART's identifiers include: 1) facial images; 2) fingerprints; 3) iris images; 4) palm prints; 5) voice recordings; 6) scars, marks, and tattoos; 7) DNA or DNA profiles; and 8) "other modalities."[52] These biometric identifiers may be compiled in conjunction with biographic identifiers, such as one's full name; date of birth; gender; signature; personal physical details (*e.g.*, height, weight, eye color, and hair color); assigned number identifiers (*e.g.*, Social Security numbers and passports); identifiers for citizenship and nationality; miscellaneous officer comments; derogatory information; current and past whereabouts; and encounter data.[53] Together, this data will form "[r]ecords related to the analysis of relationship patterns among individuals and organizations that are indicative of . . . possible terrorist threats from non-obvious relationships . . . ."[54]

Upon its completion this year, HART will allow DHS to craft a truly holistic picture of an individual's personhood, life, and movements.[55]

---

[44] *See* Privacy Act of 1974, 5 U.S.C. § 552a (1974), System of Records, 83 Fed. Reg. 17829 (Apr. 24, 2018); *see also* GOV'T ACCOUNTABILITY OFFICE REPORT, *supra* note 18, at 44 (stating that the HART program's implementation has experienced delays).

[45] *See* 83 Fed. Reg. 17,829 (Apr. 24, 2018).

[46] FOIA REQUEST, *supra* note 42, at 2.

[47] *See* 83 Fed. Reg. 17,829, 17,831 (Apr. 24, 2018).

[48] *Id.* at 17,829.

[49] In re Leidos Innovations Corporation, 2018 U.S. Comp. Gen. LEXIS 80, at *2 (Jan. 18, 2018).

[50] *Id.*

[51] *See generally* 83 Fed. Reg. 17,829, 17,829–33 (Apr. 24, 2018), Jennifer Lynch, *HART: Homeland Security's Massive New Database Will Include Face Recognition, DNA, and Peoples' "Non-Obvious Relationships*", ELEC. FRONTIER FOUND. (June 7, 2018), https://www.eff.org/deeplinks/2018/06/hart-homeland-securitys-massive-new-database-will-include-face-recognition-dna-and.

[52] 83 Fed. Reg. 17,829, at 17,831 (Apr. 24, 2018).

[53] *Id.* at 17,829, 17,831.

[54] *Id.* at 17,833.

[55] *See, e.g., Border Security, Commerce, and Travel: Commissioner Mcleenan's Vision for the Future of CBP: Hearing Before the Subcomm. on Border & Maritime Sec. of the H. Comm. on Homeland Sec.*, 115th Cong. 26 (2018) (statement of Kevin K. McAleenan, Commissioner, Customs & Border Protection) ("A comprehensive entry/exit system that leverages both biographic and biometric data . . . will make it

President Trump's Executive Order, Expedited Completion of the Biometric Entry-Exit Tracking System, further mandates that DHS seek "social media identification data and . . . social media user credentials, such as passwords to Facebook accounts of refugees and visa applicants."[56] Because of its scope and interest in the personal lives of its targets, the Entry-Exit Tracking System may lay the groundwork for future big data surveillance that "attempts to assess criminal and terroristic risk across entire populations and subpopulations . . . ."[57] With this in mind, the aforementioned biographic, biometric, and social media identifiers should raise serious questions as to the scope of the federal government's authority to profile and surveil U.S. persons.

III. BASES FOR BIOMETRIC DATA COLLECTION & THEIR LIMITS

A. AUTHORIZATION OF BIOMETRIC COLLECTION THROUGH THE HOMELAND SECURITY ACT OF 2002

Leaving aside the development of DHS's collection endeavors, the agency has two purported legal bases for its biometric data collection. The more recent of the two is the Homeland Security Act of 2002,[58] which first heralded IDENT's expansion beyond its initial function as a mere fingerprint database at the border.[59] The 2002 Act explicitly directed DHS to "develop technologies" and "store information relevant to any of its law enforcement, border, or national security functions."[60] Then, in 2004, the "9/11 Commission . . . recommended the adoption of a 'biometrics-based entry-exit system' at the nation's border" to help detect criminals and suspected terrorists entering the U.S. through airports.[61] Even so, the scope of early entry-exit detection programs was limited to foreign nationals—not U.S. citizens—and was principally concerned with "visa overstay travel fraud" rather than the formation of holistic integrated biometric databases.[62]

---

possible to confirm the identity of travelers at any point in their travel . . . ."), https://www.govinfo.gov/content/pkg/CHRG-115hhrg30900/pdf/CHRG-115hhrg30900.pdf.

[56] Margaret Hu, *Algorithmic Jim Crow*, 86 FORDHAM L. REV. 633, 640–41 (2017).

[57] *Id*.

[58] Homeland Security Act of 2002, 6 U.S.C. § 121 (2002) (directing the Secretary of Homeland Security to "take reasonable steps to ensure that information systems and databases of the Department are compatible with each other and with appropriate databases of other Departments").

[59] *See* Donohue, *supra* note 10, at 465 n.323. Here, Professor Donohue succinctly lays out the statutory bases for the collection of personally identifiable information "at the most general level." *Id*. at 463. In particular, Donohue points to the Homeland Security Act of 2002, 6 U.S.C. §§ 121(a)–(d) (2006) (establishing the "Office of Intelligence and Analysis within DHS and giving it the responsibility of accessing, receiving, and analyzing law enforcement information, intelligence information, and other information from local, state, and federal agencies . . . in support of . . . the National Counterterrorism Center"). Donohue also highlights §§ 141, 121(d)(11)–(12) (2006 & Supp. IV 2011), which gives DHS "the authority to disseminate information to other federal agencies" with only extremely limited restrictions primarily relating to the protection of intelligence sources and law enforcement practices. *Id*. at 465 n.323.

[60] *Id*. at 466.

[61] HARRISON RUDOLPH ET AL., GEO. L. CTR. ON PRIVACY & TECH., NOT READY FOR TAKEOFF: FACE SCANS AT AIRPORT DEPARTURE GATES 5 (2017), https://www.airportfacescans.com/sites/default/files/Biometrics_Report__Not_Ready_For_Takeoff.pdf.

[62] *See id*. at 5–6.

Despite the enormous power vested in DHS, the Senate Homeland Security and Governmental Affairs Committee only voted in 2017 to "approve legislation authorizing the operations of the Department . . . for the first time since the Department's inception on March 1, 2003"—a full fifteen years after the Homeland Security Act of 2002.[63] During this period, both the volume and methods of data collection at the border aggressively expanded[64] (with no new congressional directive) despite the diminishing ability of foreign terrorist organizations to coordinate attacks within the United States.[65]

The Act, fully titled the Department of Homeland Security Authorization Act of 2017,[66] also placed OBIM, which oversees the collection and storage of biometric data, under DHS guidance.[67] However, despite the integration of DHS and OBIM, "Congress has repeatedly ordered the collection of biometrics from foreign nationals at the border, but has never clearly authorized the border collection of biometrics from American citizens using face recognition technology."[68] The conspicuous lack of a statutory basis for biometric data collection has led some researchers at Georgetown Law's Center on Privacy and Technology to conclude that DHS's facial recognition scanning of U.S. citizens stands on dangerously shaky legal ground.[69]

Furthermore, the Homeland Security Act of 2002 specifically tasked DHS with integrating intelligence information in the context of counterterrorism efforts.[70] Because the Homeland Security Act of 2002 was created in direct response to the external threat posed by overseas terrorist groups in the immediate aftermath of 9/11, there is a great deal of uncertainty concerning whether the purpose and intent of the Act also applies to civilian data collection outside any reasonable counterterrorism investigation.

---

[63] Jordan Brunner, *Summary: The Department of Homeland Security Authorization Act of 2017*, LAWFARE (Mar. 19, 2018, 1:23 PM), https://www.lawfareblog.com/summary-department-homeland-security-authorization-act-2017.

[64] PATRICK NEMETH, OFFICE OF BIOMETRIC IDENTITY MGMT., DEP'T OF HOMELAND SEC., IDENTITY APPLICATIONS FOR HOMELAND SECURITY 6 (2017), https://www.eff.org/document/dhs-identity-applications-homeland-security-slide-presentation-91217.

[65] Telephone interview by Jonathan Masters with Bruce Hoffman, Senior Fellow for Counterterrorism and Homeland Sec., & Peter Bergen, Vice President and Dir., Int'l Sec., Future of War, and Global Studies and Fellows Programs, New Am. (Nov. 2, 2018), https://www.cfr.org/conference-calls/real-terrorist-threat-america.

> Since 9/11, no foreign terrorist group has successfully conducted a deadly attack in the United States . . . . So, you know, if you conceptualize the problem as a bunch of foreigners trying to attack us, which is how the—clearly how the president thinks about it, that's about seventeen years out of date. *Id*.

[66] Department of Homeland Security Authorization Act, H.R. 2825, 115th Cong. (2017).

[67] *Id*. at § 1602.

[68] RUDOLPH ET AL., *supra* note 61, at 2.

> We request that DHS stop the expansion of [the biometric data exit program] and provide Congress with its explicit statutory authority to use and expand a biometric exit program on U.S. citizens. If there is no specific authorization, then we request an explanation for why DHS believes it has the authority to proceed without Congressional approval.

Letter from Senators Edward Markey & Mike Lee to Kirstjen Nielson, Secretary, Dep't of Homeland Sec. (Dec. 21, 2017), https://www.markey.senate.gov/imo/media/doc/DHS%20Biometrics%20Markey%20Lee%20letter.pdf.

[69] *Id*.

[70] Homeland Security Act of 2002, 6 U.S.C. §§ 121(d)(1)(A)–(C). The responsibilities of the Under Secretary for Intelligence and Analysis are to: (1) "identify and assess the nature and scope of *terrorist* threats to the homeland"; (2) "detect and identify threats of *terrorism* against the United States"; and (3) "understand such threats in light of actual and potential vulnerabilities of the homeland." *Id*. (emphasis added).

The Homeland Security Act of 2002 makes clear that some form of data collection is part and parcel of DHS's mission to "detect and prevent illegal entry into the U.S.," as well as to conduct "vetting and credentialing [of persons of interest]."[71] That said, Congress has never explicitly authorized biometric data collection from U.S. citizens.[72] Even if it had, DHS has not yet distinguished between data collection for counterterrorism purposes as opposed to routine travel vetting. Thus, it is doubtful whether the Homeland Security Act of 2002, without more, authorizes HART.

B. THE PRIVACY ACT OF 1974: AN INSUFFICIENT SAFEGUARD

In addition to the Homeland Security Act, DHS points to the Privacy Act of 1974[73] in its "Notice of a New System of Records" to validate its mass biometric data collection.[74] The Privacy Act "govern[s] the means by which Federal Government agencies collect, maintain, use, and disseminate individuals' records."[75] Principally, the Act limits the ways that an agency may aggregate and disseminate computerized comparisons of records, or "matching programs."[76] In other words, the government generally may not compile databases of individually identifying information and then share that data with other agencies or persons without the consent of the person whose records the agency holds.[77] In essence, this is the very purpose of HART. So, is the case closed? In short, no. The Privacy Act carves out an exception for agencies to share "individually identif[ying]" information with other agencies for law enforcement purposes.[78] The question then becomes: is HART a sufficiently tailored law enforcement database?

HART clearly functions with both law enforcement[79] and national security purposes.[80] But these functions do not comprise the totality of the data collected. And therein lies the legal issue with HART: it is an unbelievably massive database of immutable traits with suspected terrorists, drug smugglers, visa overstayers, asylum seekers, U.S. travelers, and suspicionless persons all housed under the same roof.[81] Unfortunately, the opaque and secretive nature of how the HART system collects and

---

[71] *Biometrics*, *supra* note 14.

[72] *See* Brunner, *supra* note 63.

[73] Privacy Act of 1974, 5 U.S.C. § 552a (1974).

[74] *See id*.; System of Records, 83 Fed. Reg. 17829, 17830 (Apr. 24, 2018).

[75] *Id*.

[76] 5 U.S.C. § 552a(a)(8)(A) (1974).

[77] *See id*.; *see also* DOROTHY GLANCY, PROFESSOR, SANTA CLARA UNIV. SCH. OF L., PRIVACY ACT OF 1974: BIOMETRIC RESEARCH DATABASES AND THE PRIVACY ACT OF 1974, PRESENTATION AT THE CONFERENCE "IMPROVING BIOMETRIC AND FORENSIC TECHNOLOGY: THE FUTURE OF RESEARCH DATASETS" (Jan. 26, 2015), https://www.nist.gov/sites/default/files/documents/forensics/Glancy-Presentation.pdf.

[78] 5 U.S.C. § 552a(a)(8)(B)(iii) (1974).

[79] *See, e.g*., Donohue, *supra* note 10, at 465–66.

[80] Privacy Act of 1974, 5 U.S.C. § 552a (1974); System of Records, 83 Fed. Reg. 17829, 17833 (Apr. 24, 2018).

[81] *See* Lynch, *supra* note 51 ("DHS is not taking necessary steps with its new HART database to determine whether its own data and the data collected from its external partners are sufficiently accurate to prevent innocent people from being identified as criminal suspects, immigration law violators, or terrorists."); *see also The Second Wave*, *supra* note 19, at 1127 (discussing the array of persons whose data may be stored in IDENT).

aggregates data[82] means parsing out its legitimate law enforcement function from illegal collection and storage is nearly impossible. Thus, although the Privacy Act establishes some general rules for record collection and retention, it cannot adequately safeguard individuals' privacy rights for the following reasons.

First, the Act only safeguards the privacy interests of U.S. citizens and permanent residents and does not set boundaries for local and state government actors who share their records with DHS.[83] Thus, in what may be a glaring loophole within privacy rights, an "agency using such data is only subject to the much weaker expectation of due diligence and is under no statutory obligation to inform the individual that personally identifiable information has been collected on the target or to correct any errors in the same."[84] Furthermore, the Privacy Act also allows agencies to store and maintain the biometric data of American citizens who were non-citizens at the time of collection.

Second, storing mounds of personally-identifying data in one place has predictably allured hackers regardless of how the government collects and stores the data. In 2015, for example, the federal government's own Office of Personnel Management was the victim of a massive data breach that compromised fingerprints of 5.6 million federal employees.[85] However, internal threats might be just as destructive. Even the staunchest pro-biometric collection advocates acknowledge that careless or rogue individuals within the government (both local and federal) who have access to systems like HART could abuse the system's consolidated nature for their own personal gain.[86] This inherent weakness is only exacerbated by the fact that DHS has outsourced development of the HART system to Northrop Grumman, a private sector security firm, which must now be relied upon to collect and store billions of immutable data points without the same regulations and oversight required of federal agencies.[87]

Third, agencies often utilize a notice of proposed rulemaking to attempt to exempt their biometric data collection mechanisms from provisions of the Privacy Act. DHS, for example, issued a notice to exempt the HART system from the "notification, access, and amendment procedures of the Privacy

---

[82] *See generally* Cheri Kiesecker, *Big Gov Meet Big Brother? The U.S. Race to Beat China*, MO. EDUC. WATCHDOG (Oct. 25, 2018), http://missourieducationwatchdog.com/big-gov-meet-big-brother-the-u-s-race-to-beat-china/.

[83] *See* Donohue, *supra* note 10, at 468. The issue is also raised that many immigrants' and asylum seekers' biometric data remains in the IDENT system even long after they gain American citizenship.

[84] *Id*. at 471.

[85] Andrea Peterson, *OPM Says 5.6 Million Fingerprints Stolen in Cyberattack, Five Times as Many as Previously Thought*, WASH. POST (Sept. 23, 2015), https://www.washingtonpost.com/news/the-switch/wp/2015/09/23/opm-now-says-more-than-five-million-fingerprints-compromised-in-breaches/?utm_term=.9d7d6b81858d; *accord* Michael Riley et al., *Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It*, BLOOMBERG (Mar. 17, 2014, 10:31 AM), https://www.bloomberg.com/news/articles/2014-03-13/target-missed-warnings-in-epic-hack-of-credit-card-data.

[86] ELLISON ET AL., *supra* note 21, at 8.

[87] *Northrop Grumman Wins $95 Million Award from Department of Homeland Security to Develop Next-Generation Biometric Identification Services System*, NORTHROP GRUMMAN: NEWSROOM (Feb. 26, 2018), https://news.northropgrumman.com/news/releases/northrop-grumman-wins-95-million-award-from-department-of-homeland-security-to-develop-next-generation-biometric-identification-services-system.

Act, and consequently the Judicial Redress Act."[88] This burgeoning problem may "obliterate any substantive impact that the Privacy Act might otherwise have on this rapidly-emerging field."[89] For this reason, some biometric data collection systems could develop entirely beyond the reach of the Privacy Act's protections—even if it means U.S. citizens could be targeted without recourse.[90] It is an icy irony that DHS's attempts to circumvent the Privacy Act's "notification, access, and amendment procedures" fly in the face of the Homeland Security Act, which requires that DHS officials "treat information in such databases in a manner that complies with applicable Federal law on privacy."[91]

Lastly, the drafters of the Privacy Act—adopted over forty-five years ago—could not have fully foreseen the widespread biometric data-gathering and computing technologies currently at agencies' disposal. In fact, the Privacy Act was passed in an era before the Internet and even cellular phones, much less smart phones.[92] Despite this, even in 1974, the drafters of the Act specifically identified biometrics as an area to keep an eye on due to heightened privacy concerns.[93]

In sum, the Homeland Security Act likely authorizes mass data collection of non-U.S. persons. But, while the Homeland Security Act and Privacy Act do not preclude collection of citizens' biometric data, they certainly do not authorize such collection. Additionally, as currently interpreted by DHS, the statutes are rife with privacy loopholes and do not provide a mechanism for redress for overcollection or misuse of immutable data.

IV. THE INTEGRATION OF BIOMETRIC & BIOGRAPHIC DATA

For the reasons given above, there is reason to believe that DHS's unfettered biometric data collection supposedly authorized by the Homeland Security Act does not fully grasp the marked shift in the collection of biometric identifiers that has taken place post-9/11. The transition from IDENT to HART signaled more expansive collection, new modalities, streamlined information sharing, and increased surveillance in more spheres of one's life.[94] However, it is the intersection of immutable biometric data with extensive biographic identifiers that enables a greater "level of intrusiveness [that] suggests something different in kind, not degree, from what has come before."[95] As Judge Ginsburg wrote in *United States v. Maynard*,

---

[88] Privacy Act of 1974, 5 U.S.C. § 552a (1974); System of Records, 83 Fed. Reg. 17829, 17833 (Apr. 24, 2018).

[89] Donohue, *supra* note 10, at 472.

[90] *Id*. (discussing how the CIA is not required to provide individuals access to the records taken from them, is not required to reveal whether an individual's data is within the database and need not establish procedures allowing individuals to contest the content of those records).

[91] Homeland Security Act of 2002, 6 U.S.C. §121(d)(15)(B) (2002).

[92] GLANCY, *supra* note 77.

[93] *Id*.

[94] *See supra* accompanying text and notes 42–50.

[95] Donohue, *supra* note 10, at 410.

> A person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups—and not just one such fact about a person, but all such facts.[96]

Such "mosaics" of personal, identifying information portend further privacy incursions and necessitate a more comprehensive standard to regulate biometric data collection. Again, it has been over forty-five years since the Privacy Act of 1974. During that period, collectable identifiers expanded from simple fingerprint sheets to include voice data, retinal scans, facial recognition technology, video recordings, location data, and much more.[97] When these intrusive biometric technologies are paired together, they may "allow[] governments to observe and record actions in public space and to recall this information for any number of reasons. Such remote tracking . . . requires no suspicion of any individual; it functions as warrantless mass surveillance . . . [and] has perfect recall."[98]

For these reasons, privacy rights advocates fear that facial scan technology deployed in public spaces will "chill free speech and thwart free association" wherever it is implemented.[99] In fact, even DHS's Privacy Impact Assessment for facial scanning used in airports on U.S. citizens admits that the only way to avoid having one's personal biometric data collected "is to refrain from traveling" at all.[100] If passengers do not submit to mandatory facial scans that collect and store their personal data, then they "may be denied boarding."[101] The same impact assessment attempts to mitigate these concerns by stating that individuals may file a request to access their data through a Freedom of Information Act request or through the Privacy Act.[102] However, as mentioned in Section III.B., DHS subsequently filed a request to exempt facial scans and other biometric records stored in the HART database from those exact "notification, access, and amendment procedures."[103] Because of these repeated exemption requests, there is every reason to believe that the duplicitous nature of DHS's privacy assurances are nothing more than doublespeak designed to lull travelers into a false sense of agency over their data's collection, storage, and use.

The government's ability to identify and track individuals through their biometric data, even without suspicion that a crime has been or will be committed, should be cause for concern. A prime example of the deleterious consequences of unfettered profile-building and tracking is the infamous

---

[96] 615 F.3d 544, 562 (D.C. Cir. 2010).

[97] *See* Privacy Act of 1974, 5 U.S.C. § 552a (1974); System of Records, 83 Fed. Reg. 17829, 17830 (Apr. 24, 2018).

[98] Donohue, *supra* note 10, at 409.

[99] RUDOLPH ET AL., *supra* note 61, at 14.

[100] U.S. DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT UPDATE FOR THE TRAVELER VERIFICATION SERVICE (TVS): PARTNER PROCESS 9 (June 12, 2017), https://www.dhs.gov/sites/default/files/publications/privacy-piacbp030-tvs-june2017.pdf.

[101] *Id*.

[102] *Id*.

[103] Privacy Act of 1974, 5 U.S.C. § 552a (1974); System of Records, 83 Fed. Reg. 17,829, 17,833 (Apr. 24, 2018).

New York Police Department (NYPD) report, "Radicalization in the West: The Homegrown Threat," which was produced in 2007 as a manual for using biographic and relationship data to surveil Muslim communities.[104] The NYPD report warned that "enclaves of ethnic populations that are largely Muslim often serve as 'ideological sanctuaries' for the seeds of radical thought."[105] The NYPD then used biometric and biographic data as heuristics for criminal activity:

> The NYPD watche[d] "'radicalization incubators'—mosques, cafes, cab driver hangouts, flophouses . . . student associations, nongovernmental organizations, hookah bars, butcher shops, and book stores." Most egregiously, it identifie[d] as "radicalization indicators" the wearing of traditional Islamic clothing, beard growth, alcohol abstention, and "becoming involved in social activism and community issues,"—all of which are First Amendment-protected activities, and none of which inherently indicate criminality or terroristic activity.[106]

Not only did the NYPD report chill protected speech and expression, it also failed to "generate even a single lead" in over ten years.[107]

Functionally, the NYPD report gathered data on U.S. citizens, aggregated biometric and biographic data to form individualized profiles, tracked the whereabout of U.S. citizens, and used the aforementioned data to extrapolate interpersonal relationships and even beliefs.[108] But, rather than ensure a safer community, it only led to consternation and distrust. Unfortunately, the parallels between the NYPD report and the DHS HART database and entry-exit programs are uncanny. Like the NYPD program, HART will collect data on U.S. citizens, is designed to integrate biographic and biometric data into holistic profiles, will store records of individuals' location data, and will seek to ascertain "non-obvious relationships" from this data.[109] From this information alone, it is evident that HART may be ripe for abuse as a weapon against ethnic, religious, or political minorities.

V. A BRIEF FOURTH AMENDMENT ANALYSIS

The Fourth Amendment provides: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . . ."[110] In *Katz v. United States*, the

---

[104] *See generally* THE N.Y.C. POLICE DEP'T, RADICALIZATION IN THE WEST: THE HOMEGROWN THREAT (2007), https://sethgodin.typepad.com/seths_blog/files/NYPD_Report-Radicalization_in_the_West.pdf.

[105] *Id*. at 22.

[106] Carlos Torres, Azadeh Shahshahani & Tye Tavaras, *Indiscriminate Power: Racial Profiling and Surveillance Since 9/11*, 18 U. PA. J.L. & SOC. CHANGE 283, 292–93 (2015).

[107] *NYPD Shuts Down Controversial Muslim Surveillance Program*, HOMELAND SEC. NEWS WIRE (Apr. 18, 2014), http://www.homelandsecuritynewswire.com/dr20140418-nypd-shuts-down-controversial-muslim-surveillance-program.

[108] *See supra* accompanying text and notes 94–96.

[109] *See* Privacy Act of 1974, 5 U.S.C. § 552a (1974); System of Records, 83 Fed. Reg. 17829, 17833 (Apr. 24, 2018).

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

Supreme Court laid the groundwork for modern Fourth Amendment jurisprudence, affirming that "the Fourth Amendment protects people, not places."[111] Those "people" to whom Fourth Amendment considerations are due are "The People" enshrined in the Constitution,[112] which consists of U.S. citizens and non-U.S. persons with significant voluntary connections to the United States.[113] The Fourth Amendment, then, prohibits unlawful searches and seizures where a person has a reasonable expectation of privacy. Katz also "announced a two-part test to determine whether a person has a reasonable expectation of privacy, which assesses (1) whether the person exhibited an actual, subjective expectation of privacy and (2) whether that expectation is one that society recognizes as reasonable."[114]

As in criminal law, national security "[s]urveillance regimes often involve several stages: first, the acquisition of information; second, the analysis of that information; and third, the use or disclosure of that information. Fourth Amendment law traditionally has focused only on the first step—the acquisition of information."[115] Despite this, the Fourth Amendment has not yet been extended to the government's biometric data acquisition within the national security sphere.[116] That should change.

Although a significant portion of HART's biometric data collection likely occurs at the border, not all of it does.[117] Thus, the HART system should be split into at least two separate databases segmented by 1) acquisitions at the border versus those away from the border, and 2) by modality, the type of data collected.[118] Despite the fact that no cases have yet challenged the HART system—possibly because it has not yet been fully implemented—there are several recent decisions that seem to buttress privacy advocates' hopes for more robust data protection.

A. FOURTH AMENDMENT AWAY FROM THE BORDER

Traditionally, courts have granted the highest deference to the government when national security interests are at stake.[119] Yet what constitutes a national security interest is not always clear, especially when, as is the case here, the searches at issue are diverse in location, source, target, and kind.[120] The government has a strong argument that a database is necessary to identify suspected terrorists entering the U.S., but should that same system and same justification apply to parents seeking adoptions

[111] Katz v. United States, 389 U.S. 347, 351 (1967).

[112] U.S. CONST. pmbl.

[113] United States v. Verdugo-Urquidez, 494 U.S. 259, 271 (1990) (requiring that aliens have "significant voluntary connection[s]" with the U.S. to trigger Fourth Amendment protections).

[114] Kristine Hamann & Rachel Smith, *Facial Recognition Technology: Where Will It Take Us?,* AM. BAR ASS'N, https://www.americanbar.org/groups/criminal_justice/publications/criminal-justice-magazine/2019/spring/facial-recognition-technology/ (last visited May 21, 2019) (citing Katz v. United States, 389 U.S. 347 (1967)).

[115] Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 331–32 (2012).

[116] *See* Carpenter v. United States, 138 S. Ct. 2206, 2210 (2018).

[117] *See The Second Wave*, *supra* note 19.

[118] *See supra* accompanying text and notes 91–93.

[119] *See infra* accompanying text and note 139 (discussing the Mathews v. Eldridge balancing test).

[120] Not only is national security a catch-all term, but it also can be used to justify biometric data collection even in the absence of evidence that there is a problem at all. For example, when researchers at Georgetown Law Center reviewed data on the Biometric Entry-Exit Program they concluded that it was a "solution in search of a problem." RUDOLPH ET AL., *supra* note 61, at 5.

nowhere near a border or port of entry?[121] Should it also apply to facial recognition scanning of U.S. citizens traveling into or out of the U.S.?[122]

Most recently, the Supreme Court found in *Carpenter v. United States* that warrantless acquisition of location data was an unlawful search in violation of the Fourth Amendment.[123] Though that decision intentionally avoided the issue of national security, it might signal a future willingness to address the issue. For example, Chief Justice Roberts's opinion expressed an understanding of the ballooning reach of technology when he stated, "[T]he Court is obligated—as '[s]ubtler and more far-reaching means of invading privacy have become available to the Government'—to ensure that the 'progress of science' does not erode Fourth Amendment protections."[124]

The central issue in *Carpenter* was whether chronicling an individual's past movements constituted a Fourth Amendment violation.[125] There, the Court found that this "chronicling" of information required that the government possess probable cause to conduct the search.[126] In fact, "[t]he Court usually requires 'some quantum of individualized suspicion' before a search or seizure may take place."[127] In contrast to the requirement of "individualized suspicion," many of the individuals whose biometrics are stored in IDENT and will be stored in the HART system are completely suspicionless despite DHS's efforts to chronicle their past locations and movements. But *Carpenter* also indicated that the Court may be wary of coupling facial recognition technology with other identifiers[128] and hinted that "compiling data across various databases (whether public or private), throughout multiple locations over a long period, may also implicate the Fourth Amendment."[129]

As mentioned in Part IV, in *Maynard*, Judge Ginsburg argued that the mosaic principle should apply to Fourth Amendment cases that reveal a person's movements.[130] The mosaic principle is a legal theory that contends that surveillance or collection should trigger Fourth Amendment protections when individual points of datum, taken together, create a "mosaic" of a person's life.[131] Because HART seeks to form holistic profiles and even keeps record of previous movements,[132] it is plausible that the system records "an intimate picture of the subject's life"[133] that may trigger Fourth Amendment protections.

---

[121] *The Second Wave*, *supra* note 19, at 1127 (stating that DHS collects data on both suspected terrorists and prospective parents seeking overseas adoptions).

[122] *See generally* RUDOLPH ET AL., *supra* note 61 (discussing the fact that DHS has never been granted statutory permission to use facial recognition technology on U.S. citizens).

[123] *See* 138 S. Ct. 2206, 2210–11. It is unclear whether courts will find that data stored on an electronic device parallels personally identifying biometric data. *See generally* Riley v. California, 573 U.S. 373 (2014) (holding that the "police generally may not, without a warrant, search digital information on a cell phone seized from an individual who has been arrested").

[124] 138 S. Ct. 2206, at 2223 (quoting Olmstead v. United States, 277 U.S. 438, 473–74 (1928)).

[125] *Id*. at 2216.

[126] *Id*. at 2221.

[127] *Id*. (quoting United States v. Martinez-Fuerte, 428 U.S. 543, 560–61 (1976)).

[128] *Id*. at 2212–21; *see* United States v. Jones, 565 U.S. 400 (2012) (Sotomayor, J., concurring).

[129] Hamann, *supra* note 114.

[130] United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010).

[131] *See generally* Kerr, *supra* note 115 (discussing and defining the mosaic theory).

[132] *See* ELLISON ET AL., *supra* note 21, at 3–4 (stating that HART stores biographic data that includes records of past and present location data).

[133] 615 F.3d, at 563.

In sum, there is a strong Fourth Amendment argument that the government requires probable cause and individualized suspicion for biometric collection not at the border, but it may not ultimately win the day because of past hesitancy to apply the Fourth Amendment to national security issues. Ultimately, this issue may continue to persist until either HART's collection methods become less opaque or "national security" is limited as a catch-all interest.

B. FOURTH AMENDMENT AT THE BORDER

At the border, however, the "[t]he Government's interest in preventing the entry of unwanted persons and effects is at its zenith . . . ."[134] That said, according to the Ninth Circuit decision in *United States v. Cotterman*, "[t]his does not mean . . . that at the border 'anything goes.'"[135] Instead, "[e]ven at the border, individual privacy rights are not abandoned but '[b]alanced against the sovereign's interests.'"[136]

In *Cotterman*, the Court found that a reasonableness analysis that considered the totality of the circumstances was appropriate—even at the border—when the search at issue was forensic in nature.[137] Though the sovereign's interest at the border is great, the privacy rights language in *Cotterman* leaves a narrow door open for plaintiffs to argue that HART collection constituted a Fourth Amendment violation, especially if it is a suspicionless person.

If, even at the border, "privacy rights are not abandoned,"[138] then "national security" as a catch-all rationale may break down when confronted with the privacy rights of individuals coerced into divulging large amounts of personally-identifying data. That said, this appears to be a bleak argument if and until there is a successful challenge to DHS's collection of biometric data of U.S. persons at the border. For this reason, I propose that DHS divide HART into separately maintained sub-systems: first, by the person whose data is collected; second, by the type of data collected; and third, by the location that the data was obtained (i.e., at the border or not).

VI. A NEW APPROACH: CONGRESS SHOULD ENACT STANDARDS & AN INDEPENDENT RIGHT OF ACTION FOR DATA MISUSE

Whether or not courts find that the Fourth Amendment constrains biometric collection of suspicionless persons' identifiers, Congress should pass a new biometric privacy law to regulate biometric data collection in the digital age. In particular, the suggested law should clearly delineate what types of biometric data may be collected, how the data should be stored, when it will be destroyed, from whom it will be taken, why it is being taken, and how to request access to one's own stored data. On access, the suggested law should carve out a narrow private right of action by which an individual

---

[134] United States v. Flores-Montano, 541 U.S. 149, 152 (2004).
[135] 709 F.3d 952, 960 (2013) (quoting United States v. Seljan, 547 F.3d 993, 1000 (2008)).
[136] *Id*. (quoting United States v. Montoya de Hernandez, 473 U.S. 531, 539 (1985)).
[137] *Id*. at 962.
[138] *Id*. at 960.

may: (1) view the data attributed to them in the HART database; and/or (2) challenge their status as a "national security threat" and enjoin DHS from storing his or her data without suspicion that a crime has been or will be committed.

Privacy rights advocates will argue that a right of action is the surest way to secure the fundamental right to privacy.[139] HART's intermingling of multiple private and immutable biometric modalities with biographic data and quasi-public social media data[140] will, inevitably, chill speech and expression.[141] This leaves the following question:

> [W]hat is the value of privacy? Privacy creates a framework that allows other values to exist and develop. Where privacy is available, we can have freedom, liberty, and other intrinsic goods. . . . If [personal] information is used abusively, similar to how we might feel if we were filmed all the time, it compromises our ability to act naturally and freely.[142]

Where a government's commitment to respecting privacy is questioned, it follows that the community's trust in that government will erode.[143]

Critics of a private right of action will respond threefold. First, the government might have legitimate reasons as to why an individual whose biometric data is stored in HART should not know his or her data is kept in the database (i.e., he or she is a national security threat) and, thus, not be able to access that data. Courts have consistently applied the *Matthews v. Eldridge* balancing test,[144] which weighs the private interest against erroneous deprivations against the government's strong interest in ensuring national security, and usually side with the government. Second, a private right of action will open up agencies to burdensome litigation, which will cost taxpayers millions as agencies must spend time and resources defending suits. Finally, one might respond that if you have not done anything wrong, then you should have nothing to hide.[145] Broad biometric databases, even of suspicionless individuals, help solve crimes and promote security.

Ultimately, these objections are unpersuasive. First, it is unreasonable to house biometric data for suspected terrorists, lawful immigrants, asylum seekers, routine travelers, and parents seeking an adoption all within the same umbrella database. The HART system is overly broad and necessarily

---

[139] Olmstead v. United States, 277 U.S. 438, 478–79 (1928).

> They conferred, as against the Government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment. *Id*. (Brandeis, J., dissenting).

[140] Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) ("A person does not surrender all Fourth Amendment protection by venturing into the public sphere. To the contrary, 'what [one] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.'") (quoting Katz v. United States, 389 U.S. 347, 351 (1967)).

[141] Matthew Sundquist, *Online Privacy Protection: Protecting Privacy, The Social Contract, and the Rule of Law in the Virtual World*, 25 REGENT U. L. REV. 153, 158 (2012).

[142] *Id*.

[143] *See The Second Wave*, *supra* note 19, at 1155.

[144] *See generally* 424 U.S. 319 (1976) (establishing that alleged due process violations require consideration of the individual's interest, the government's interest, and any administrative burdens).

[145] Sundquist, *supra* note 141, at 158–59.

stores millions of pieces of biometric data of suspicionless U.S. citizens. As a consequence, HART and other "big data" databases "can assign a heightened suspicion and facilitate inferences of guilt."[146] Second, burdensome litigation should not be a concern so long as the right is sufficiently narrowly tailored. Using the DHS Traveler Redress Inquiry Program[147] as a guide, the majority of inquiries could be handled online without any adjudication. Finally, having "nothing to hide" is a red herring. The very fact that personal identifying data is taken is, itself, a harm. That data could also be stolen and used against its owner, which is all the more dangerous because of its immutability. One may procure a new driver's license but not a new voice or new irises.

An example of good collection practices is the use of biometrics by the International Criminal Police Organisation (INTERPOL).[148] Even though INTERPOL engages in extensive counterterrorism efforts, it stores only three types of modalities (face, fingerprints, and DNA) in three separate databases,[149] which mitigates the possibility of forming holistic personal profiles of suspicionless persons. The internal governance and operation of the databases is overseen by an independent body that also provides a remedy for individuals who object to their data being stored in INTERPOL's database.[150]

To ensure data privacy while safeguarding national security, Congress should act to regulate HART and update the Privacy Act. To effectively balance privacy rights against the government's interest in national security, I recommend the following statutory provisions. First, the statute should amend the Homeland Security Act to delineate between counterterrorism and law enforcement-related collection versus collection of suspicionless U.S. persons' data. Second, the statute should update the Privacy Act's protection of biometric data to bring it into the 21st century. Third, the statute should outline which specific identifiers DHS may collect depending on the target—asylum seekers, suspected terrorists, and parents adopting a child should not all be subject to the same litmus test. Fourth, the HART system should be split into multiple systems to separate threats to national security from suspicionless persons. Fifth, the number and types of modalities collected should depend on the target, which will allow the government to maintain holistic profiles on suspected terrorists while limiting the profiles that can be constructed on suspicionless citizens. Sixth, following INTERPOL, the statute should provide for a narrow right of action to enable individuals to uncover whether HART houses their data and to request its removal. Finally, the statute should establish an independent body to oversee data collection and set a timeline for the data's destruction once individuals are found to no longer constitute a national security threat. With these

[146] Margaret Hu, *Big Data Blacklisting*, 67 FLA. L. REV. 1735, 1776 (2015).

[147] *DHS Traveler Redress Inquiry Program*, TRANSP. SEC. ADMIN., https://www.tsa.gov/travel/passenger-support/travel-redress-program.

[148] U.N. Office of Counter-Terrorism & U.N. Security Council Counter-Terrorism Committee Executive Directorate, *Compendium of Recommended Practices for the Responsible Use and Sharing of Biometrics in Counter-Terrorism*, at 63–64 (2018).

[149] *Id*.

[150] *Id*. at 64.

protections, personal privacy may be maintained while still allowing DHS to effectively safeguard national security.

In conclusion, the HART system raises serious data privacy questions due to the exponential growth of biometric identification technologies. Although the Fourth Amendment may provide some protections, the surest course of action would be for Congress to update the Privacy Act and set boundaries on the current state of uninhibited biometrics collection.