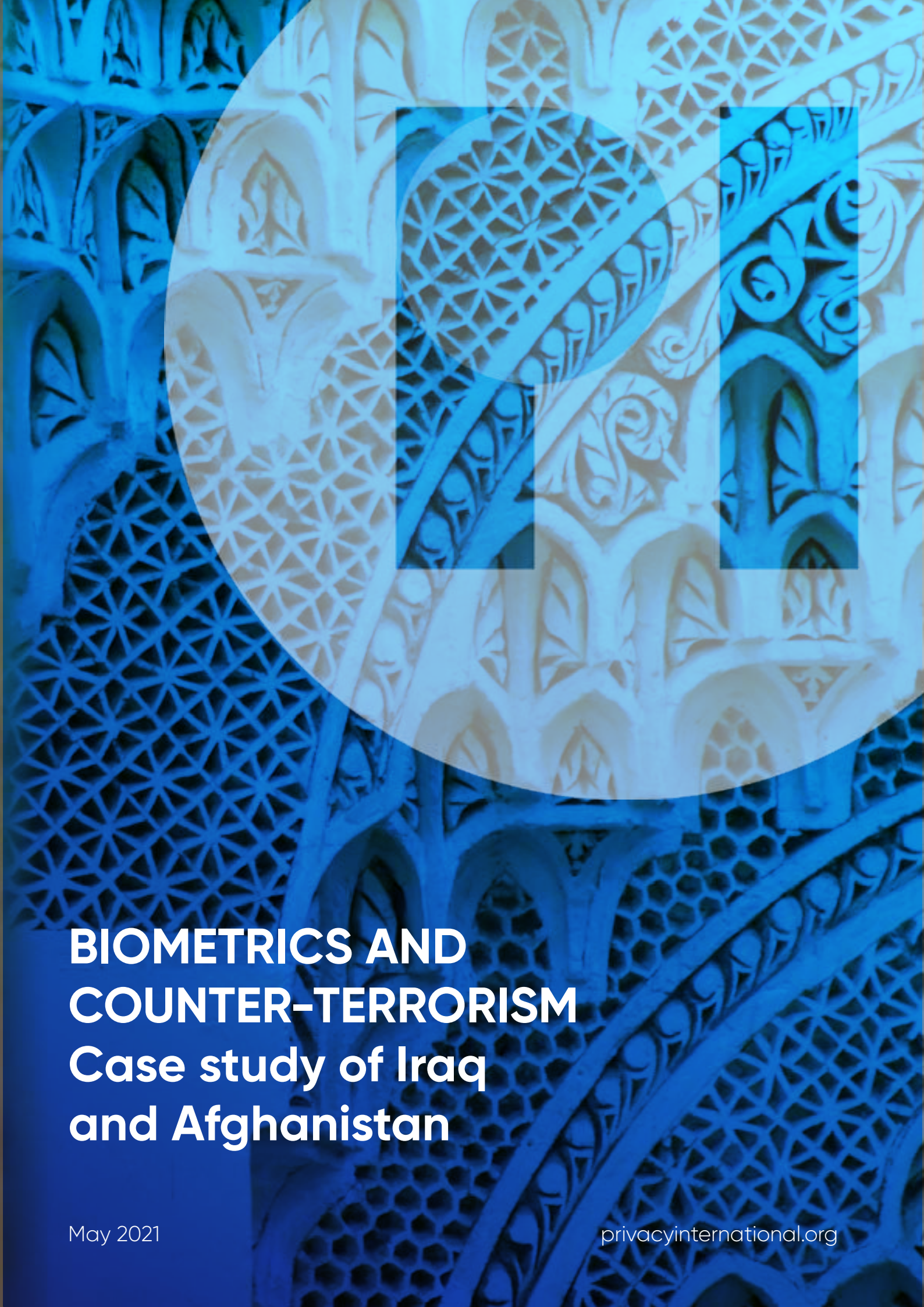


BIOMETRICS AND COUNTER-TERRORISM
Case study of Iraq and Afghanistan

May 2021

privacyinternational.org

Author

This report was compiled by Nina Toft Djanegara, PhD Student, Department of Anthropology, Stanford University, in collaboration with Privacy International

ABOUT PRIVACY INTERNATIONAL

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

So, join our global movement today and fight for what really matters: our freedom to be human.

Open access. Some rights reserved.

Privacy International wants to encourage the circulation of its work as widely as possible while retaining the copyright. Privacy International has an open access policy which enables anyone to access its content online without charge. Anyone can download, save, perform or distribute this work in any format, including translation, without written permission. This is subject to the terms of the Creative Commons Licence Deed: Attribution-Non-Commercial-No Derivative Works 2.0 UK: England & Wales. Its main conditions are:

- You are free to copy, distribute, display and perform the work;
- You must give the original author ('Privacy International') credit;
- You may not use this work for commercial purposes;

You are welcome to ask Privacy International for permission to use this work for purposes other than those covered by the licence.

Privacy International is grateful to Creative Commons for its work and its approach to copyright. For more information please go to www.creativecommons.org.

Privacy International
62 Britton Street, London EC1M 5UY, United Kingdom
Phone +44 (0)20 3422 4321
privacyinternational.org

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

Cover image: Photo by عين الله في on Unsplash

CONTENTS

ABOUT THIS REPORT 3

OVERVIEW **5**

TIMELINE 9

IRAQ 10

AFGHANISTAN 12

KEY CONCERNS RELATED TO DESIGN AND IMPLEMENTATION **16**

DATA SHARING 18

RECENT USAGE OF BIOMETRICS BY
THE U.S. DEPARTMENT OF DEFENSE 22

CONTRACTORS, HARDWARE PROVIDERS, AND IT SERVICES 24

CONCLUSION **26**

ABOUT THIS REPORT

Biometrics has become closely linked to counter-terrorism. Indeed, in 2017 the UN Security Council Resolution 2396 placed a binding obligation on member states to "develop and implement systems to collect biometric data … in order to responsibly and properly identify terrorists, including foreign terrorist fighters."[1] Similarly, the argument for the deployment of biometrics on counter-terrorism grounds is recurring in support of national identity systems: from the UK's aborted scheme in the mid-2000s through to the recent developments in Kenya.

However, the human rights implications of these technologies have been brought into question. As the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism wrote in 2020: "in the absence of robust rights protections which are institutionally embedded to oversee collection, storage, and use of such evidence, relevant practices are likely to infringe international human rights law standards."[2]

[1] See Privacy International's response on this topic: https://privacyinternational.org/advocacy/3066/briefing-un-counter-terrorism-executive-directorate-biometric-data.

[2] Krisztina Huszti-Orbán and Fionnuala Ní Aoláin, *The Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business?* Report prepared under the aegis of the Mandate of the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism (University of Minnesota Human Rights Center, 2020), https://www.law.umn.edu/sites/law.umn.edu/files/2020/07/21/hrc-biometrics-report-july2020.pdf.

To better understand the impact of these systems, it is worthwhile to turn back the clock to one of the key moments in the development of these technologies: the "War on Terror" and the use of biometrics by the US military in Afghanistan and Iraq. While not the first time that biometrics had been proposed as a counter-terrorism tool, the post-9/11 use of these technologies is deeply informative.

The following case study is the result of an extensive survey of government documents, military field manuals, industry reports, journalistic sources, and academic literature. This research revealed important insights about the *ad hoc* nature of the military biometrics program in its early years and its indiscriminate data collection practices in Afghanistan and Iraq. The rationale justifying the introduction of these technologies is also telling: biometrics became a key tool of war and identity was reframed as a matter of national security. Or, as one operation manual put it, the aim was achieving "identity dominance": "The operational capability to achieve an advantage over an adversary by denying him the ability to mask his identity and/or to counter biometric technologies and processes."[3]

[3] U.S. Army Commander's Guide to Biometrics in Afghanistan", Report from *Center for Army Lessons Learned*, April 2011, https://publicintelligence.net/call-afghan-biometrics/.

OVERVIEW

The U.S. Department of Defense (DOD) first explored applications for biometric technology in the late 1990s, when it began utilizing biometric identification to manage logistics and personnel, as well as restrict access to secured facilities[4]. However, it was not until after the terrorist attacks of 11 September 2001 that the DOD biometrics program began in earnest and its focus was shifted to counter-terrorism.

The DOD biometric program developed in confluence with US military operations in Afghanistan and Iraq. Its expansion was tightly linked to the goals of military commanders during the "War on Terror": to distinguish insurgents and terrorists from the local civilian population[5]. Detecting adversaries and "denying anonymity" became a matter of national security. That is to say, Iraq and Afghanistan were not merely sites where biometric information was collected; the DOD's biometrics policies and practices represented a political and policy shift, which set precedent for more recent intelligence and counter-terrorism

[4] "Biometrics Task Force Annual Report FY09" Department of Defense Report, 2009, https://fas.org/man/eprint/biometric09.pdf.

[5] "Biometrics in Government Post-9/11", Report by the National Science and Technology Council, September 2008, https://fas.org/irp/eprint/biometrics.pdf; see also William C. Buhrow, *Biometrics in Support of Military Operations: Lessons from the Battlefield*, Routledge, 2016, https://www.routledge.com/Biometrics-in-Support-of-Military-Operations-Lessons-from-the-Battlefield/Buhrow/p/book/9781482260212.

operations, such as the collection of biometric data from suspected ISIS fighters and affiliates in Raqqa[6].

After testing biometric prototypes in Afghanistan in 2002 and in Iraqi detention centers in 2003, the Department eventually mandated that fingerprints, facial photographs, and DNA must be collected from all of its detainees worldwide[7]. To collect and store this data, the DOD launched its Automated Biometric Identification System (ABIS) in 2004, a database that serves as a central repository for all biometric data collected by the military. Entries in the ABIS database adhere, for the most part, to the 13-point biometric standard (10 fingerprints, 2 iris scans, 1 facial photograph)[8]. DOD policy states that this biometric data "will be stored indefinitely in support of the War on Terrorism.[9]" The Department of Defense also operates a Biometrically Enabled Watchlist (BEWL), which links the biometric and biographic information for certain persons of interest whose inclusion on the watchlist has been determined by intelligence analysts. According to the U.S. Government Accountability Office (GAO), in the decade between 2008 and 2017, DOD biometric data had contributed to the capture of 1,700 people and denied 92,000 people access to US military bases; furthermore, 213,000 people had been placed on the Biometrically Enabled Watchlist[10].

---

[6] "Scrambling to Track Islamic State Terrorists, Coalition Turns to Biometrics", *VOA News,* November 2017, https://www.voanews.com/middle-east/scrambling-track-islamic-state-terrorists-coalition-turns-biometrics; see also "Defeated in Syria, ISIS Fighters Held in Camps Still Pose a Threat", *New York Times*, January 2018, https://www.nytimes.com/2018/01/24/world/middleeast/isis-syria-militants-kurds.html.

[7] "Department of Defense Biometric Standards Development Recommended Approach", DOD Report from Biometrics Management Office, September 2004, Homeland Security Digital Library, https://www.hsdl.org/?view&did=449571.

[8] Glenn Voelz, *Rise of iWar: Identity, Information, and the Individualization of Modern Warfare*, Strategic Studies Institute, 2015, https://www.hsdl.org/?abstract&did=788293.

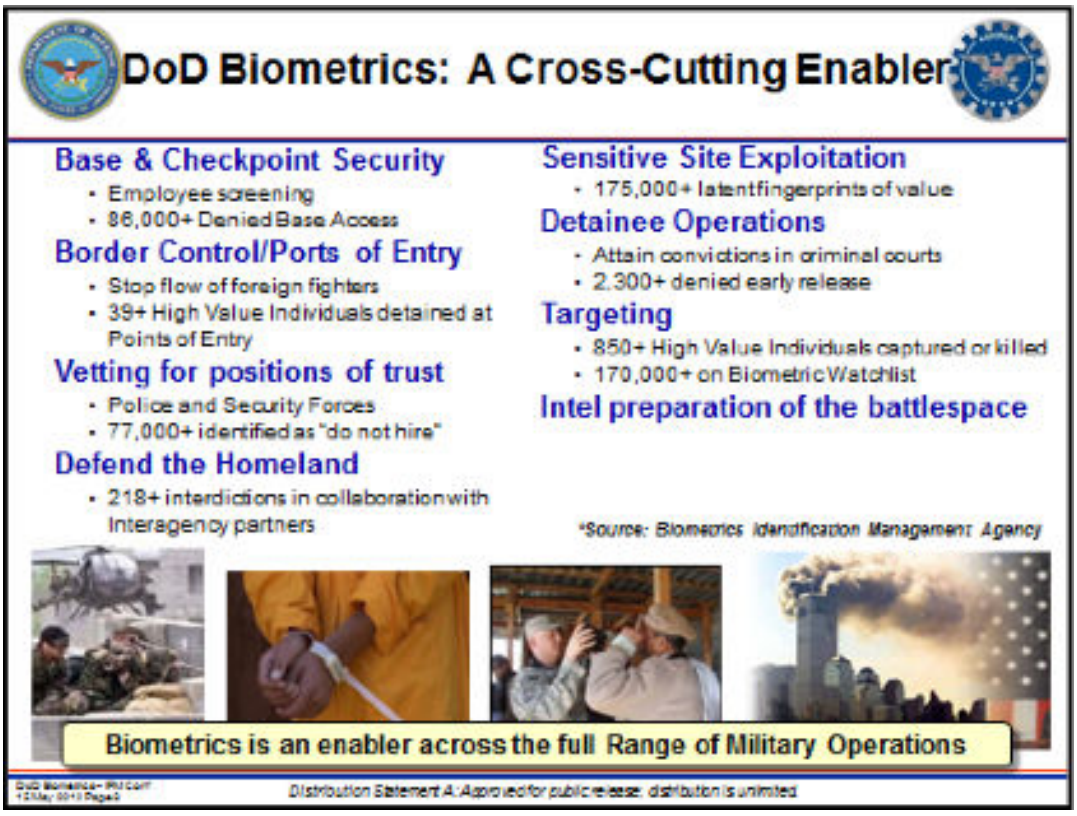
[9] "DoD Policy for Biometric Information for Access to U.S. Installations and Facilities in Iraq", Memorandum for Secretaries of the Military Departments, July 2005, https://fas.org/sgp/othergov/dod/biometric.pdf.

[10] "Progress Made in Establishing Long-term Deployable Capabilities, but Further Actions Are Needed", United States Government Accountability Office (GAO) Report, August 2017, https://www.gao.gov/assets/690/686416.pdf.

The majority of the ABIS database is comprised of identities collected from people in Iraq and Afghanistan: detainees, prisoners of war, people applying to work on US military bases or the Iraqi police, recipients of microloans[11], and anyone whose identity could be considered a national security concern. This latter category is rather broad and undefined, leading some critics to question what they characterize as the DOD's dragnet approach. Glenn Krizay, the Director of the Defense Forensics and Biometrics Agency, recently remarked that the ABIS database even includes biometric information from voter enrollments, government personnel records, and military enlistments in partner countries. He emphasized, "What's important is that DoD is collecting in austere places other parts of the federal government generally are not."[12]

[11] "U.S. ramps up biometrics to ID Baghdad residents", *Homeland Security Newswire*, May 2008, http://www.homelandsecuritynewswire.com/us-ramps-biometrics-id-baghdad-residents.

[12] "Draft Director's Outline for 18 Jun 2019 Annual Identity Management Symposium", Presentation notes for Glenn Krizay, Director of the Defense Forensics and Biometrics Agency, June 2019, Obtained by OneZero via FOIA request, https://www.scribd.com/document/433613080/Presentation-notes-from-Glenn-Krizay-director-of-the-Defense-Forensics-and-Biometrics-Agency-June-2019#download&from_embed.

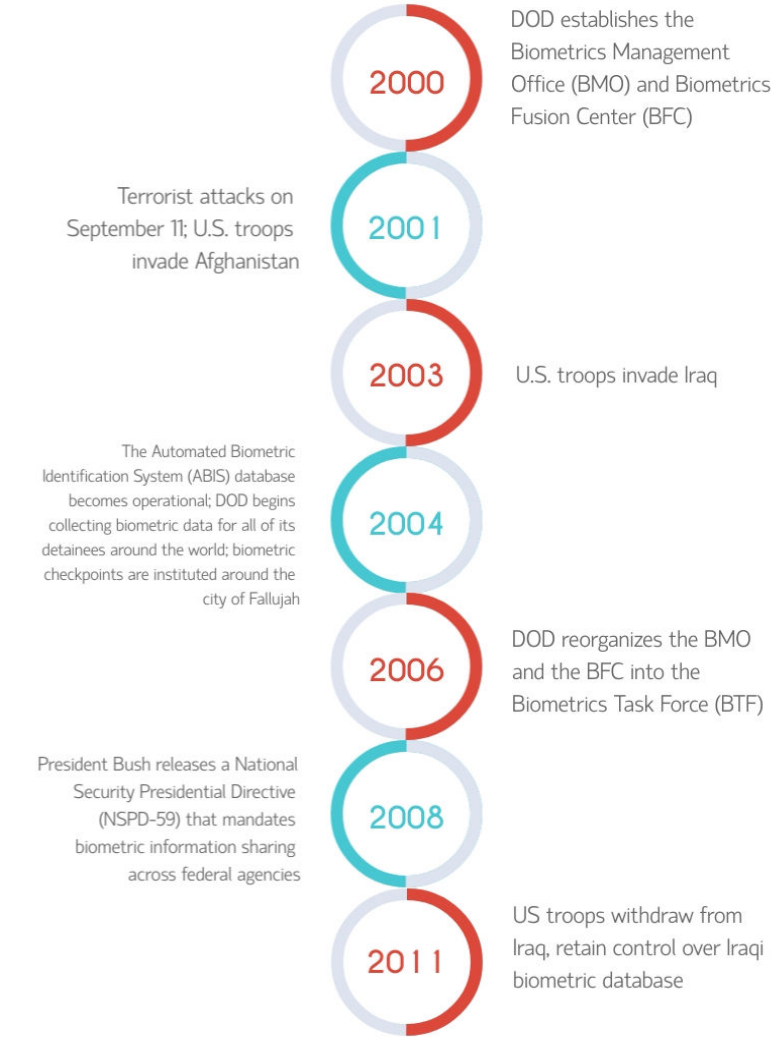


A slide from a 2012 presentation by Dalton Jones, Defense Intelligence Agency (DIA) Senior Expert for Biometrics, illustrates the various purposes for which the US military makes use of biometrics. [13]

[13] "Identity Intelligence-From Reactionary Support to Sustained Enabler", Presentation slides by Dalton Jones, DIA Senior Expert for Biometrics, August 2012, https://fas.org/irp/eprint/i2-dia-2012.pdf.

TIMELINE:

Key dates in U.S. military biometrics



IRAQ

In late 2004, insurgents rose up against US forces and took control of Fallujah. After US troops regained control of the city, in what would eventually be known as the bloodiest battle of the Iraq War[14], they forcibly evacuated over 200,000 people and established checkpoints surrounding the perimeter. In an effort to ensure that outside fighters were not attempting to re-infiltrate the city, US forces required all "military-aged male" residents to register for a biometric ID card before they were permitted to reenter Fallujah[15].

Biometric data collection subsequently expanded to the wider Anbar province and Baghdad, where *USA Today* reported that US troops were stopping people at "checkpoints, workplaces and sites where attacks have recently occurred" and enrolling them in the biometric database; moreover, in certain neighborhoods surrounding Baghdad "troops have gone door to door collecting data."[16] In response to the *USA Today* article, Privacy International co-signed a letter to the Department of Defense, along with the Electronic Privacy Information Center (EPIC) and Human Rights Watch, expressing concern about the lack of privacy measures and the potential for misuse if the data were to fall into the wrong hands due to the history of ethnic conflict in the region[17].

---

[14] Dan Lamothe, "Remembering the Iraq War's Bloodiest Battle, 10 Years Later", *Washington Post*, 4 November 2014, https://www.washingtonpost.com/news/checkpoint/wp/2014/11/04/remembering-the-iraq-wars-bloodiest-battle-10-years-later/.

[15] William C. Buhrow, *Biometrics in Support of Military Operations: Lessons from the Battlefield*, Routledge, 2016, https://www.routledge.com/Biometrics-in-Support-of-Military-Operations-Lessons-from-the-Battlefield/Buhrow/p/book/9781482260212; see also "Iraq Diary: Fallujah's Biometric Gates", *Wired,* August 2007, https://www.wired.com/2007/08/fallujah-pics/.

[16] "U.S. is building database on Iraqis", *USA Today*, June 2007, https://usatoday30.usatoday.com/news/world/iraq/2007-07-12-iraq-database_N.htm.

[17] "US Biometric Identity System of Iraqis", Letter to DOD from EPIC, PI, and HRW, July 2007, https://www.epic.org/privacy/biometrics/epic_iraq_dtbs.pdf.

US military forces also provided the Iraqi government with biometrics and forensic technology in a bid to strengthen local rule of law and prosecute terrorists within the Iraqi criminal justice system[18]. In cooperation with the Iraqi government, they established an Automated Fingerprint Identification System to screen applicants to the Iraqi police force and digitized fingerprints from 280,000 criminal records[19]. The biometric data collected by the Iraqi government was also transmitted to the ABIS database in West Virginia[20].

After retreating from Iraq in 2011, U.S. Central Command confirmed that it would continue to maintain control over its biometric database, which by this time contained the identities of 3 million Iraqis[21]. In an interview with *Wired* magazine, Army Major T.G. Taylor justified the retention of the database thusly: "We have this information, and rather than cull through it all and say 'bad guy, good guy, bad guy, good guy, it's better to just keep it, because that would be very time consuming…Biometric data was collected on people who worked on the bases. You're a good guy; you worked here. It's not like we're collecting [data] on an enemy."[22] While Taylor's statement characterizes the work of analysing the data as inordinately time consuming, DOD reports indicate that the national intelligence community was actively engaged in exactly this sort of analysis when populating the Biometrically Enabled Watchlist[23].

---

[18] "A Systems Approach to Biometrics in the Military Domain", *Journal of Forensic Sciences,* November 2018, https://pubmed.ncbi.nlm.nih.gov/29464706/.

[19] "The Role of Biometrics in the Counterinsurgency", Transcript of "Department of Defense Bloggers Roundtable" conversation with Lieutenant Colonel John W. Velliquette Jr., Iraqi Biometrics Manager, August 2007, http://www.epic.org/privacy/biometrics/blog_transcript.doc.

[20] *Ibid.*

[21] "U.S. Holds on to Biometrics Database of 3 Million Iraqis", *Wired,* December 2011, https://www.wired.com/2011/12/iraq-biometrics-database/.

[22] *Ibid.*

[23] "Biometrics-Enabled Intelligence", Department of Army report, November 2015, https://fas.org/irp/doddir/army/atp2-22-82.pdf.

AFGHANISTAN

Building off its use of biometrics in Iraq, the US military began similar efforts in Afghanistan. In Afghanistan, biometric information was collected from suspected insurgents, dead[24] and live enemy combatants, detainees, military contractors, applicants seeking to join the Afghan police or army, as well as other individuals. Additionally, as reported in 2010, the DOD began integrating its forensic and biometric capabilities, lifting latent fingerprints from improvised explosive devices (IEDs), weapons, and documents and entering them into the ABIS database[25].

Recommendations in the "U.S. Army Commander's Guide to Biometrics in Afghanistan" [26] advise military officials to integrate biometrics collection into all of their operations, to "create a sense of urgency" around biometrics collection, and "be creative and persistent in their efforts to enroll as many Afghans as possible". These guidelines were taken to heart at the national border, where US forces arbitrarily stopped and biometrically registered people coming into Afghanistan; by 2011, randomly selected border crossers made up 10% of all biometric enrolments in Afghanistan[27]. In areas with high insurgent activity, all "military-aged males" were compulsorily registered. *The Economist* reported that Afghani men were being pulled out of mosques, their homes, and public transportation in order to have their fingerprints and irises scanned[28]. According

[24] "The eyes have it", *The Economist,* July 2012, https://www.economist.com/asia/2012/07/07/the-eyes-have-it.

[25] "US army amasses biometric data in Afghanistan", *The Guardian*, October 2010, https://www.theguardian.com/world/2010/oct/27/us-army-biometric-data-afghanistan.

[26] "U.S. Army Commander's Guide to Biometrics in Afghanistan", Report from *Center for Army Lessons Learned*, April 2011, https://publicintelligence.net/call-afghan-biometrics/.

[27] "Afghanistan Has Big Plans for Biometric Data", *New York Times*, November 2011, https://www.nytimes.com/2011/11/20/world/asia/in-afghanistan-big-plans-to-gather-biometric-data.html?pagewanted=all.

[28] "The eyes have it", *The Economist,* July 2012, https://www.economist.com/asia/2012/07/07/the-eyes-have-it.

to an article in *Wired*, the US military has "gathered data on almost every Afghan it comes in regular contact with,[29]" while the *New York Times* commented that "A citizen in Afghanistan or Iraq would almost have to spend every minute in a home village and never seek government services to avoid ever crossing paths with a biometric system."[30] These journalistic reports depict a biometric collection program that enrolled millions of Afghans under situations of coercion and/or where consent was unlikely to be free and informed.

The "U.S. Army Commander's Guide to Biometrics in Afghanistan" [31] recommended that biometric and biographic information should be logged for all persons living in operational areas. However, the Guide acknowledges that people might be hesitant to provide their personal information and that units might face "a general aversion to mass involuntary enrollments". To this end, the Guide urged military commanders to frame biometric enrollment as a matter of "protecting their people" and "mak[ing] them safer" in order to win support from tribal leaders and village elders. For instance, the Guide advises that "The message can be crafted that the census is intended to protect them from the influence of outsiders and will give them a chance to more easily identify troublemakers in their midst." Similarly, former army intelligence officer William C. Buhrow has disclosed some of the tactics used to convince local leaders to endorse biometric data collection. He explains:

> *"U.S. forces operating in both Iraq and Afghanistan found it very useful to engage with local leadership and the local security or militia forces in planning for biometrics collections. In fact, we were sometimes able to convince local village leaders that collecting biometrics on military-aged males in their villages and providing those enrolled with some kind of*

[29] "Marines Land in Afghanistan — With Biometrics", *Wired*, May 2008, https://www.wired.com/2008/05/marines-land-in-afghanistan-with-biometrics/.

[30] "To Track Militants, U.S. Has System That Never Forgets a Face", *New York Times,* July 2011, https://www.nytimes.com/2011/07/14/world/asia/14identity.html.

[31] "U.S. Army Commander's Guide to Biometrics in Afghanistan", Report from *Center for Army Lessons Learned*, April 2011, https://publicintelligence.net/call-afghan-biometrics/.

> *identity card could help deter outsiders from entering their villages and disrupting the local power structure (or making the village a possible target for future kinetic operations by U.S. or Coalition forces). The bottom line is that it is always better to involve local officials or security elements in biometrics collections than to go it alone. Providing an incentive to cooperate (or a disincentive, if they do not cooperate) can be very useful in securing local cooperation."*[32]

Assisted by US funding and training, the Afghan government also initiated its own biometric registration program. The Afghan government collected biometric data from passport and driver license applications, university students, soldiers, and public officials with the intention of eventually building a biometric national ID card. [33] As of 2020, this ambition has not yet been realized, although the current Afghan administration is continuing its efforts, looking to India's controversial/privacy invasive Aadhar program for guidance[34]. The risks posed by the development of biometric databases in Afghanistan were starkly illustrated when local journalists reported in 2016 and 2017 that Taliban insurgents were stopping busses and using biometric scanners to identify and execute any passengers who were determined to be security force members[35]. While the US encouraged the Afghan government to build its own biometric

[32] William C. Buhrow, Biometrics in Support of Military Operations: Lessons from the Battlefield, Routledge, 2016, https://www.routledge.com/Biometrics-in-Support-of-Military-Operations-Lessons-from-the-Battlefield/Buhrow/p/book/9781482260212.

[33] "Afghanistan Has Big Plans for Biometric Data", *New York Times*, November 2011, https://www.nytimes.com/2011/11/20/world/asia/in-afghanistan-big-plans-to-gather-biometric-data.html?pagewanted=all.

[34] "Afghanistan seeks India's help to build national biometric database", *Biometric Update,* January 2020, https://www.biometricupdate.com/202001/afghanistan-seeks-indias-help-to-build-national-biometric-database.

[35] "Taliban Used Biometric System During Kunduz Kidnapping", *TOLO News,* June 2016, https://tolonews.com/afghanistan/taliban-used-biometric-system-during-kunduz-kidnapping; see also "Taliban subject passengers to biometric screening", *Pajhwok Afghan News*, February 2017, https://www.pajhwok.com/en/2017/02/14/taliban-subject-passengers-biometric-screening; Ali Karimi, "Surveillance in Weak States: The Problem of Population Information in Afghanistan", *International Journal of Communication*, 2019, https://ijoc.org/index.php/ijoc/article/view/9803.

database of its citizens and provided material support[36], it is unclear whether US officials offered training or assistance on data security principles.

[36] "U.S. Army Commander's Guide to Biometrics in Afghanistan", Report from *Center for Army Lessons Learned*, April 2011, https://publicintelligence.net/call-afghan-biometrics/.

KEY CONCERNS RELATED TO DESIGN AND IMPLEMENTATION

An internal assessment conducted by the U.S. Government Accountability Office (GAO) in 2008 concluded that the DOD had not issued sufficient guidance for data collection procedures during "field activities where US forces encounter hostile or questionable individuals such as in Afghanistan and Iraq."[37] Subsequent GAO assessments identified further gaps in DOD policies and implementation of standards. In one instance, DOD officials justified the continued use of a device that did not meet its own technical standards because "it was developed as an urgent mission need for Central Command to collect and authenticate the identity of individuals."[38]

The DOD's lack of adherence to its own standards reveals the ad-hoc nature of the biometrics program, which began operations before clearly defining roles and responsibilities or engaging in long-term planning. The Partnership for Public Service, a private think tank in Washington D.C., made a similar assessment of the DOD biometrics program, which they characterized as "whipped up quickly" as "the Army rapidly purchased whatever companies had available," hastened by the easy accessibility of funding during wartime. [39] The Partnership for Public Services identified a number of concerns in regards to the Army's use of biometrics, including insufficient training and mismatched technology. These reports paint a portrait of a biometrics program that was put together quickly

[37] "DOD Can Establish More Guidance for Biometrics Collection and Explore Broader Data Sharing", United States Government Accountability Office (GAO) Report, October 2008, https://www.gao.gov/new.items/d0949.pdf.

[38] "DOD Can Better Conform to Standards and Share Biometric Information with Federal Agencies", United States Government Accountability Office (GAO) Report, March 2011, https://www.gao.gov/assets/320/317368.pdf.

[39] "From Data to Decisions III: Lessons from Early Analytics Programs", Report by think tank *Partnership for Public Service*, November 2013, http://www.businessofgovernment.org/sites/default/files/From%20Data%20to%20Decisions%20III.pdf.

and encouraged indiscriminate data collection with no prior privacy impact assessment and little regard to developing standards and safeguards for the use, storage and deletion of biometric records[40]. For instance, as of 2009, the Biometrics Task Force was still "developing a Privacy Assurance Plan and staffing a "Privacy Interests of Non-U.S. Persons" policy," even though by that time the DOD had been regularly collecting biometric data for at least 5 years[41].

A redacted 2015 Department of Army report obtained under the Freedom of Information Act (FOIA) provides unique insight into the US military's priorities in regard to biometrics-enabled intelligence.[42] The report frames the local population as potentially hostile by default, regardless of whether any suspicious activity has been observed. Following the logic that any local person may represent a future threat, officials encouraged large-scale enrollment in the biometric database, advising that enrollment should be integrated into day-to-day operations, including traffic control, village support, checkpoints, and daily patrol. The report explains:

> *"Enrolling detainees and key segments of the local population as the tactical situation permits not only allows for better control of detained personnel but also facilitates the later identification of people who may become hostile. Conducting increased enrollments and identifications also provides for the security of the local populace by demonstrating the ability to positively identify individuals across time and space regardless of their method of disguise."*[43]

[40] "Biometrics-Enabled Intelligence", Department of Army report, November 2015, https://fas.org/irp/doddir/army/atp2-22-82.pdf.

[41] "Biometrics Task Force Annual Report FY09" Department of Defense Report, 2009, https://fas.org/man/eprint/biometric09.pdf.

[42] "Biometrics-Enabled Intelligence", Department of Army report, November 2015, https://fas.org/irp/doddir/army/atp2-22-82.pdf.

[43] *Ibid.*, 19.

The report also discloses that, "ABIS is the authoritative repository for biometric samples. Authoritative should not be construed as perfect – ABIS does report false positives."[44] A "false positive" suggests that a person may be incorrectly identified as someone whose information had previously been recorded in the database. This becomes even more concerning when considering that the database includes latent prints found in forensic investigations, which are often incomplete. However, a positive match against ABIS records can have serious consequences for the person in question[45]. For instance, *The Economist* reported in 2012 that "It is easy to come across Afghans who claim that they were wrongly denied foreign visas or jobs after a biometric scan flagged up their presence on some watchlist. Evidence held against them is rarely divulged, nor is it clear how they can challenge it."[46]

DATA SHARING

A 2008 Presidential Directive required that all US federal agencies share biometric data for "persons for whom there is an articulable and reasonable basis for suspicion that they pose a threat to national security."[47] This directive emphasized the need to "collect, store, use, analyze, and share biometrics to identify and screen KSTs [*Known and Suspected* Terrorists]."[48] In accordance with this mandate, the Department of Defense's ABIS database is linked with databases operated by the FBI and the Department of Homeland Security

[44] *Ibid.*, 37.

[45] See the case of Naif Abdulaziz M. Alfallaj detailed on page 11 of this report.

[46] "The eyes have it", *The Economist,* July 2012, https://www.economist.com/asia/2012/07/07/the-eyes-have-it.

[47] "Biometrics for Identification and Screening to Enhance National Security", National Security Presidential Directive (NSPD) 59, June 2008, https://fas.org/irp/offdocs/nspd/nspd-59.html.

[48] *Ibid.*

(DHS). The FBI Integrated Automated Fingerprint Identification System (IAFIS) database holds domestic criminal records while the DHS Automate Biometric Identification System (IDENT) is used for customs and border patrol, immigration, and visa approval. The linkage of these databases means that the US military is able to search against the biometric data of US citizens and residents. Indeed, Pentagon officials report that they have cross-checked and successfully matched the fingerprints of Iraqi detainees with criminal records in the United States[49]. The interlinked databases also enable the Department of Homeland Security to deny entry to travelers seeking to enter the United States on the basis of biometric data collected in Afghanistan or Iraq[50].

Numerous US government reports include hypothetical scenarios to illustrate the importance of biometric data sharing between federal agencies. The following excerpt from the Report of the Defense Science Board Task Force on Defense Biometrics offers one such scenario, which also depicts the workflow and travel of information between agencies:

> *"A squad on a patrol is attacked by armed plainclothes fighters. After the initial skirmish, the fighters surrender their arms and are detained by US military forces. A search of the subjects' possessions reveals falsified identification documents from Iraq, Afghanistan, and Pakistan. Biometric samples are collected from each of the detainees and are transmitted to a DoD authoritative source. The data is compared against all files within the authoritative source and a positive match is made on two of the individuals. Match results indicate these two subject's biometrics had been found at a location containing bomb-making materials in Yemen around*

[49] "FBI Prepares Vast Database Of Biometrics", December 2007, *Washington Post,* https://www.washingtonpost.com/wp-dyn/content/article/2007/12/21/AR2007122102544.html.

[50] "Biometrics Task Force Annual Report FY09", DoD report, 2009, https://fas.org/man/eprint/biometric09.pdf; see also "DOD Automated Biometric Identification System (ABIS)", Military Report, 2014, https://www.dote.osd.mil/Portals/97/pub/reports/FY2014/army/2014dodabis.pdf?ver=2019-08-22-110519-453.

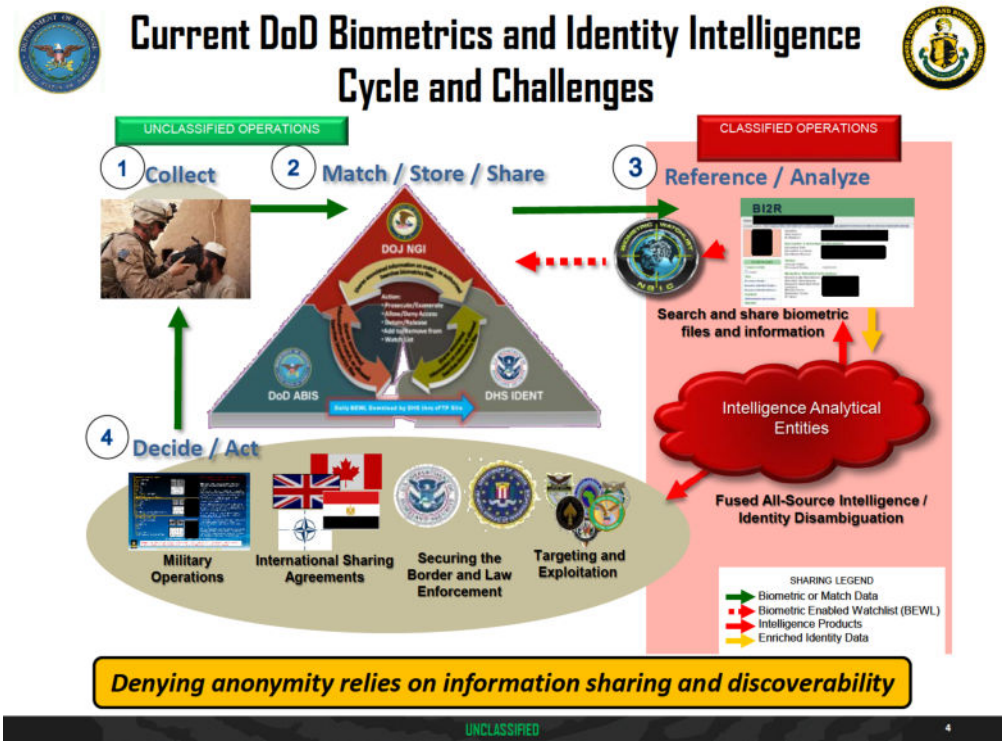
the time of the USS Cole attack. After updating and storing the subjects' new biometric files, the DoD shares all of the biometric samples and associated information with the Federal Bureau of Investigation's (FBI) biometric database, which in turn also automatically shares the files and associated information with the Department of Homeland Security (DHS). After analysis of available biometric and associated information, the subjects are nominated and promoted by the National Counter-terrorism Center (NCTC) as Known or Suspected Terrorists. The subjects' biometric files are flagged and linked to the NCTC's terrorist watch list at the DoD Authoritative Source, as well as entered into the FBI's Known or Suspected Terrorist (KST) database. Several months later, the detainees are released to a foreign government for adjudication and repatriation. Several years later, a US police department responds to a trespassing complaint at a local water treatment plant, which services a large metropolitan area. Two subjects are apprehended and fingerprints are taken at the police department's primary booking station. The fingerprints are transmitted to the FBI's fingerprint database and matches are made against the previously shared biometrics files collected from the military detainees. Because the fingerprints have been entered into the FBI's KST file, the FBI CJIS Division Intelligence Group immediately alerts the Terrorist Screening Center (TSC) of the encounter. Upon notification, the TSC advises the local Joint Terrorism Task Force to investigate whether the trespassing act was an indication of a terrorist threat to the nation."[51]

DOD officials have also emphasized the importance of data-sharing and partnerships with other national governments for counter-terrorism and "theater security cooperation" activities in order to stabilize the political situation in the Middle East. The US has biometric data sharing agreements with dozens of countries[52]. However, US biometrics policies have sometimes been at odds with

[51] "Report of the Defense Science Board Task Force on Defense Biometrics", Report by the Office of the Under Secretary of Defense For Acquisition, Technology, and Logistics, March 2007, https://fas.org/irp/agency/dod/dsb/biometrics.pdf.

[52] "The eyes have it", *The Economist,* July 2012, https://www.economist.com/asia/2012/07/07/the-eyes-have-it.

those of other nation-states. Former army intelligence officer William C. Buhrow, who was a member of the Biometrics Task Force in both Iraq and Afghanistan recounted that "European allies" took issue with the U.S. approach to biometric data. He states, "[S]ome of our ISAF [International Security Assistance Force] allies had significant constraints, both cultural and legal, to sharing or even collecting biometrics data from foreign persons. A number of our European allies also had privacy and legal policies (some less formal than others) that made them extremely hesitant to collect biometrics from Afghans and to share their collected information with U.S. forces, if that data might also be used by U.S. law enforcement or intelligence agencies.[53]"



A slide from a 2019 presentation by Glenn Krizay, Director of the Defense Forensics and Biometrics Agency, depicts the DOD's approach to information sharing[1]

[53] William C. Buhrow, Biometrics in Support of Military Operations: Lessons from the Battlefield, Routledge, 2016, https://www.routledge.com/Biometrics-in-Support-of-Military-Operations-Lessons-from-the-Battlefield/Buhrow/p/book/9781482260212.

RECENT USAGE BIOMETRICS BY THE U.S. DEPARTMENT OF DEFENSE

Much remains unknown about the precise content of the DOD's biometric database and the Department is deliberately opaque about its continued use. For instance, when the tech magazine *One Zero* submitted a FOIA request to the DOD in 2019 for more information about biometrics, including facial recognition, its request was denied on the grounds that "Public release would be tantamount to providing uncontrolled foreign access."[54]

This lack of transparency entails that the public is only able to get glimpses at the DOD's current use of ABIS through secondary reports. Unsurprisingly, these reports tend to provide only rather positive portrayals of biometrics for counter-terrorism than a comprehensive picture of the databases and their use. Nevertheless, these sources indicate that US databases that contain biometric records of foreign nationals collected at the start of the "War on Terror" are still in active use and that the US government is sharing this data with international partners. For instance, a 2017 memo to the EU Standing Committee on Operational Cooperation on Internal Security explains that US authorities have offered access to a platform that "enables the automatic comparison of fingerprints against US data, including battlefield data from Syria and Iraq and other conflict zones" to support the European Council's counter-terror operations[55].

[54] "This Is How the U.S. Military's Massive Facial Recognition System Works", *One Zero,* November 2019, https://onezero.medium.com/exclusive-this-is-how-the-u-s-militarys-massive-facial-recognition-system-works-bb764291b96d.

[55] "Security checks in case of irregular immigration - mapping exercise", Council of the European Union memo, March 2017, http://www.statewatch.org/news/2017/mar/eu-council-irregular-migrants-mapping-exercise-6717-17.pdf.

In February 2018, the *New York Times* reported that the FBI's counterterrorism division, is revisiting biometric data and DNA samples collected by the DOD to track down suspected terrorists on US soil[56]. In other words, the ABIS database continues to be leveraged as a resource for US counter-terrorism investigations after nearly two decades of amassing biometric data. The most recent statistics available on the DOD Defense Forensics and Biometric Agency website state that the ABIS database currently contains over 7.4 million identities[57]. It is estimated that approximately 3 millions of those entries were collected in Iraqi and over 2.5 million in Afghanistan[58].

[56] "Saudi Who Attended Qaeda Camp Is Arrested in Oklahoma" by Adam Goldman and Matt Apuzzo. *New York Times.* February 2018. https://www.nytimes.com/2018/02/06/us/naif-alfallaj-qaeda-camp-oklahoma.html; see also "Saudi Citizen Sentenced to More Than 12 Years in Prison for Concealing Attendance at Al Qaeda Training Camp and Visa Fraud". Department of Justice Office of Public Affairs. October 2019. https://www.justice.gov/opa/pr/saudi-citizen-sentenced-more-12-years-prison-concealing-attendance-al-qaeda-training-camp-and.

[57] "About DFBA", Defense Forensics and Biometric Agency homepage, https://www.dfba.mil/about/about-dfba.html.

[58] "Catalysts of military innovation: a case study of defense biometrics", Case study published by Defense Acquisition University Press, April 2016, https://go.gale.com/ps/anonymous?id=GALE%7CA454730180&sid=googleScholar&v=2.1&it=r&linkaccess=abs&issn=15536408&p=AONE&sw=w.

CONTRACTORS, HARDWARE PROVIDERS, AND IT SERVICES

- In 2007, L-1 Identity Solutions was awarded a $8.3 million contract to provide its Handheld Interagency Identity Detection Equipment (HIIDE), a biometric enrolment and recognition device designed for use in the field[59]. L-1 Identity Solutions was acquired by Safran in 2011 and presumably the contract was transferred over. In 2008, the Motorola Biometrics Business Unit also had active contracts with the U.S. Army and Iraqi National Police; the company was acquired by Safran in 2009[60]. Safran is now part of the biometrics giant IDEMIA.`
- A second handheld device, the Biometric Automate Toolset, has also been used by the US military to collect fingerprints and iris scans in the field. This device was obtained through a $159 million U.S. Army contract with the IT and hardware provider GTSI (now rebranded as UNICOM Government) and its partner Cross Match Technologies, Inc. (now rebranded as HID Global)[61].
- According to former army intelligence officer William C. Buhrow, US forces in Afghanistan and Iraq relied heavily upon contractors to staff and carry out its biometric operations, with only a few military officials in leadership

[59] "L-1 wins $8.3 million U.S. Army contract for HIIDE 4.0 biometric device", Homeland Security News Wire, March 2009, http://www.homelandsecuritynewswire.com/l-1-wins-83-million-us-army-contract-hiide-40-biometric-device.

[60] "State of the Art Biometrics Excellence Roadmap", MITRE Technical Report, October 2008, https://ucr.fbi.gov/fingerprints_biometrics/biometric-center-of-excellence/files/saber-techassessment-vol-1_14_jan.pdf.

[61] "Biometrics and National Security", White paper from Biometrics Research Group, Inc., 2014, https://www.academia.edu/7434174/Biometrics_and_National_Security.

positions. He estimated a ratio of 10 military officers to 200 contractors employed by the Biometrics Task Force in 2009[62].

- In 2006, private defense company Northrup Grumman was contracted to manage operations and provide IT support for the Automated Biometric Identification System. The contract was renewed in 2011 for $141 million[63]. As of 2018, the defense contractor ManTech has taken over technical support, infrastructure maintenance, and project management for DOD Tactical Biometrics Systems, while Leidos and Ideal Innovations manage the ABIS database[64].

[62] William C. Buhrow, Biometrics in Support of Military Operations: Lessons from the Battlefield, Routledge, 2016, https://www.routledge.com/Biometrics-in-Support-of-Military-Operations-Lessons-from-the-Battlefield/Buhrow/p/book/9781482260212.

[63] "U.S. Defense Department Selects Northrop Grumman for $141 Million Task Order to Continue Support of the Automated Biometric Identification System", Northrop Grumman Press Release, May 2011, https://investor.northropgrumman.com/news-releases/news-release-details/us-defense-department-selects-northrop-grumman-141-million-task.

[64] "PM DoD Biometrics Quick Reaction Capability (QRC) System Support", PR materials from ManTech, September 2018, https://www.mantech.com/sites/default/files/2018-09/biometrics_9_12.pdf; "This Is How the U.S. Military's Massive Facial Recognition System Works", *One Zero,* November 2019, https://onezero.medium.com/exclusive-this-is-how-the-u-s-militarys-massive-facial-recognition-system-works-bb764291b96d.

CONCLUSION

This research shows how the DOD's biometric programme was developed and implemented without prior assessment of its human rights impact and without the safeguards necessary to prevent its abuse. Its application, while on paper justified for counter-terrorism purpose, led to indiscriminate collection and storage of biometric data of millions of people in Iraq and Afghanistan, the vast majority of whom would pose not security threat. Further, the US military encouraged the collection of biometric data by national police/security authorities, again without considering the privacy and human rights implications.

The open questions that remain regarding the whereabouts and current use of the DOD's biometric programme and its reappearance in contemporary current affairs – almost twenty years after the invasion of Afghanistan – shows that there is a need to be vigilant over the impact of these systems. This biometric data has a long legacy. We must keep this in mind when deploying new biometric systems: the true impact and effect of these systems might not be felt today, but decades from now. That is why it remains imperative that the deployment of such systems must be approached with caution, with the highest standards of human rights in mind. It cannot remain a shadowy operation, dominated by secrecy and silencing dissent; only an open and informed debate can ensure that the use of biometrics for counter-terrorism does not result in unintended consequences, out of sight of the public.

Privacy International
62 Britton Street
London EC1M 5UY
United Kingdom

+44 (0)20 3422 4321

privacyinternational.org

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