REFUGEES AND THE BIOMETRIC FUTURE: THE IMPACT OF BIOMETRICS ON REFUGEES AND ASYLUM SEEKERS

Achraf Farraj*

The use of biometrics has a unique impact upon refugees and asylum seekers, and it has the potential to improve national and international efforts to protect them. Biometrics afford refugees and asylum seekers a credible means of establishing their identity, even where they lack other documentation, and likely increases the political viability of projects designed for their benefit by improving accuracy and resistance to fraud. Indeed, biometrics have been used for a variety of purposes, such as to aid humanitarian efforts by allowing interested parties to more accurately identify the size of refugee populations and more effectively deliver aid to those who need it most. However, the application of biometrics to refugees and asylum seekers raises several concerns, including violation of privacy, misidentification, stigmatization, and the potential to block meritorious asylum applications. Furthermore, to the extent that national laws may inadequately protect refugees and asylum seekers, biometric technology, owing to its usefulness in law enforcement—something which should be readily apparent in light of the long history of fingerprinting—might ultimately undermine their safety and welfare. These concerns demand that policymakers take into account the unique circumstances of refugees and asylum seekers and take steps to ensure that their well-being is in fact furthered by the collection, storage, and utilization of their biometric information. Once these concerns are addressed, however, biometrics should continue to be utilized to protect refugees and asylum seekers.

---

* JD Candidate, Columbia Law School, 2011. I would like to thank Professor Christina Burnett, Andrew Case, and Allison Khaskelis for their thoughtful comments on earlier drafts of this Note. Any errors or omissions are solely my own.

Part I begins with a brief description of biometric technology. Part II surveys various areas in which biometrics are used, including (1) assisting in the identification of asylum seekers and management of their applications for asylum, (2) facilitating refugees' freedom of movement through their incorporation into refugee travel documents, (3) helping the United Nations High Commissioner for Refugees (UNHCR) prevent fraud in refugee camps, and (4) providing states with a workable means of reducing the detention of asylum seekers. In doing so, the Note identifies both situations in which the use of biometrics has been problematic, along with those in which the increased use of biometrics would benefit refugees and asylum seekers.

Part III addresses whether the collection and retention of biometric information interferes with the privacy interests of refugees and asylum seekers. It concludes that the collection of biometric information from refugees and asylum seekers does not violate U.S. or EU privacy law. More specifically, it concludes that the U.S. policy requiring fingerprinting of asylum seekers is not an unreasonable search under the Fourth Amendment. With respect to storage of biometric information, it argues in favor of reducing the duration for which such information is stored and implementing measures to restrict the transfer of biometric information stored in databases maintained by the Department of Homeland Security (DHS) and other agencies. Part IV discusses other problematic aspects of biometrics as applied to refugees and asylum seekers, specifically the possibility of misidentification and the potential of reluctance to submit to biometric enrollment. It urges caution in the collection of biometric information and subsequent use before courts and other decisionmakers.[1]

1. In order to better assess how the use of biometrics uniquely affects refugees and asylum seekers, this Note draws upon the laws of the United States, the European Union and its Member States, and international law. Both the United States and the European Union have made considerable use of biometrics in implementing their immigration laws and policies. International law defines the rights of refugees and forms the foundation of relevant international organizations, such as the UNHCR and the International Civil Aviation Organization (ICAO).

I. INTRODUCTION

A. What Are Biometrics?

The term "biometrics" refers either to biological or physiological characteristics usable for automatic recognition or to the automated process of recognizing individuals based on such characteristics.[2] These characteristics include fingerprints, facial structures, iris or retinal patterns, and deoxyribonucleic acid (DNA).[3] The collection of biometric information from individuals is called enrollment.[4] It can take place in a variety of settings, and it need not be voluntary, such as when an individual is recorded by a camera outfitted with facial recognition technology.[5]

Recognition can take place through either authentication or identification. Authentication is the process by which a recently collected biometric is compared to a previously collected biometric obtained from the same individual. This information may either be stored in a database or held by the individual in a storage device, such as a radio frequency identification (RFID) chip embedded in a passport.[6] Identification, on the other hand, entails comparing a

2. National Science and Technology Council (NTSC), Committee on Technology, Privacy & Biometrics: Building a Conceptual Foundation 4 (2006), *available at* http://www.biometrics.gov/docs/privacy.pdf [hereinafter NTSC Report]; *see also* Office of the Inspector Gen., U.S. Dep't of Justice, Status of IDENT/IAFIS Integration 1 n.5 (2003), http://www.usdoj.gov/oig/reports/plus/e0305/Final.pdf (defining biometrics as "biological measurements unique to each person, such as fingerprints, hand geometry, facial patterns, retinal patterns, or other characteristics that are used to identify individuals").

3. *See* Rudy Ng, Note, *Catching up to our Biometric Future: Fourth Amendment Privacy Rights and Biometric Identification Technology*, 28 Hastings Comm. & Ent. L.J. 425, 428–34 (2006) (surveying several biometric modalities and assessing their constitutionality).

4. *See* NTSC Report, *supra* note 2, at 6.

5. Rebekah Thomas**,** Global Commission on International Migration (GCIM), Biometrics, International Migrants and Human Rights (Jan. 2005), http://www.unhcr.org/refworld/docid/42ce4cc14.html (describing the general impact of biometric technology on global migration) [hereinafter GCIM Report].

6. *See* Ann Cavoukian, Information and Privacy Commissioner/Ontario, Privacy and Biometrics 2 (1999), *available at* http://www.ontla.on.ca/library/repository/mon/10000/211715.pdf [hereinafter Cavoukian, Privacy and Biometrics]. RFID chips are designed to automatically emit radio waves to transmit stored information to receiving units. RFID Journal, *What is RFID*, http://www.rfidjournal.com/article/articleview/1339/1/129 (last visited Mar. 8, 2010).

recently collected biometric against all biometric information stored in a database.[7]

B. Why Are Biometrics Used?

Biometrics are used as a means of identification and authentication because of their perceived accuracy and reliability within the law enforcement community.[8] Tremendous technological improvement has increased their usefulness in this regard. For example, software that enables automatic comparison of digitized fingerprints obviates the cumbersome and labor intensive process of matching fingerprints by hand, and advances in communications allow nearly instantaneous data sharing.[9] For such reasons, biometrics have become increasingly instrumental in enforcing criminal and immigration law, detecting persons known to pose a threat to public safety and national security, and preventing fraud.[10]

C. Which Biometrics Are Used?

Fingerprints are one of the most well-known and publicized biometric modalities,[11] and a large number of refugees and asylum seekers are consequently subject to fingerprinting in a variety of contexts discussed below. Other biometric modalities will be addressed to the extent of their relevance. In this respect, it is worth noting that some countries and international organizations favor

---

7. Cavoukian, Privacy and Biometrics, *supra* note 6, at 2.

8. *See* Federal Bureau of Investigation, Fingerprint Overview, Fingerprint Identification, *available at* http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/fingerprint-overview/fingerprint-overview/view (stating "[f]ingerprints offer an infallible means of personal identification"); *see also* Federal Bureau of Investigation, *Fingerprints & Other Biometrics*, http://www.fbi.gov/about-us/cjis/fingerprints_biometrics (last visited Feb. 20, 2011) ("Fingerprints vary from person to person (even identical twins have different prints) and don't change over time. As a result, they are an effective way of identifying fugitives and helping to prove both guilt and innocence.").

9. *See* Federal Bureau of Investigation, *Integrated Automated Fingerprint Identification System Fact Sheet*, http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/iafis/iafis_facts (last modified Aug. 11, 2010) (reporting that nearly 98% of fingerprint sets submitted to the IAFIS in October 2009 were in digital format).

10. *See* GCIM Report, *supra* note 5, at 2; *see also infra* note 20 and accompanying text.

11. NTSC Report, *supra* note 2, at 13.

facial recognition[12] or iris scanning.[13] Refugees and asylum seekers may be required to submit DNA samples in criminal proceedings or to prove a familial relationship in various other contexts, but DNA has been deemed "not sufficiently automated or quick enough to be viable for use in a biometric program."[14]

II. APPLICATION OF BIOMETRICS TO REFUGEES

A. Biometrics as a Means of Verifying the Identity of Refugees and Asylum Seekers and Usage in Processing Asylum Claims

A number of states collect biometrics from non-nationals who cross their borders. One result is the creation of databases of biometric information, which in turn enables states to compare biometric data collected at a later date and thereby enforce immigration laws. The extent to which this directly impacts refugees and asylum seekers depends upon the quality of the national laws being enforced. As discussed below, the use of biometrics has sometimes facilitated the enforcement of laws that operate to deny refugees and asylum seekers their basic rights. At the same time, making use of biometrics addresses the concerns of states that host refugees and grant asylum and may thereby increase political support for programs designed to promote the welfare of refugees and asylum seekers.

1. United States

The United States makes widespread use of biometrics in identifying and verifying the identity of refugees and asylum seekers. Refugees' fingerprints are collected prior to their entry into the

12. News Release, ICAO, Biometric Identification to Provide Enhanced Security and Speedier Border Clearance for Traveling Public, PIO 09/03 (May 28, 2003), *available at* http://www.icao.int/icao/en/nr/2003/pio200309_e.pdf [hereinafter ICAO, Biometrics Announcement].

13. *See* GCIM Report, *supra* note 5, at 6 (describing the United Arab Emirates' decision to adopt iris recognition technology to prevent reentry by *persona non grata*); *see also* John Daugman, *Iris Recognition*, Am. Scientist, July 1, 2001, at 3, 4 (explaining that "irises show complex random patterns" and noting that "[t]he available evidence to date indicates that iris patterns are indeed as fixed as one's fingerprints").

14. John D. Woodward, Jr., et al., Army Biometric Applications, Identifying and Addressing Sociocultural Concerns 30 n.13 (2001).

United States, either while obtaining a visa or at a port of entry.[15] DHS operates the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) program, which collects fingerprints from nearly all international visitors to the United States, including refugees.[16] By 2007, US-VISIT had collected nearly 100 million fingerprints,[17] and its data had been used for various purposes, such as checking the identity of visa applicants against the terrorist watch list[18] and being introduced into evidence to show that aliens overstayed their visas.[19] The anticipated benefits of US-VISIT include: "[i]mproved biometric identification of foreign national travelers who may present threats to public safety and the national security of the United States," "ensuring the integrity of the United States immigration system through enhanced enforcement of immigration laws," and "reductions in fraud, undetected imposters and identity theft."[20]

Refugees' fingerprints may also be collected during their stay in the United States. The Refugees, Asylum, and Parole System (RAPS) of the U.S. Citizenship and Immigration Services (USCIS)

15. The Department of Homeland Security (DHS) altered its procedures, effective on January 18, 2009, and expanded US-VISIT to require biometric collection from persons seeking to enter the United States as refugees or asylees. DHS, Fact Sheet: Expansion of US-VISIT Procedures to Additional Travelers, http://www.dhs.gov/files/programs/gc_1231972592442.shtm (last modified Oct. 2, 2009).

16. *Id.* Those with diplomatic visas or those aged below 14 or over 79 are exempt. Department of Homeland Security, US-VISIT Enrollment Requirements, http://www.dhs.gov/files/programs/editorial_0527.shtm (last modified Mar. 9, 2010).

17. P.T. Wright, Acting Deputy Director of US-VISIT, Press Conference on the U.S. Transition to 10-Fingerprint Collection at Borders (June 25, 2007), *available at* http://useu.usmission.gov/dossiers/travel_documents/jun2507_wright_us-visit.html.

18. DHS, Privacy Impact Assessment for the Automated Biometric Identification System (IDENT) 3 (July 31, 2006), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisit_ident_final.pdf [hereinafter IDENT PIA].

19. *See* Tariq v. Keisler, 505 F.3d 650, 654, 657–58 (7th Cir. 2007) (holding that the Pakistani national's application for asylum was supported by substantial evidence. The Government had introduced the asylum application of the applicant's father, who had made no mention of the applicant's stated grounds for asylum).

20. Implementation of the United States Visitor and Immigrant Status Indicator Technology Program ("US-VISIT") Biometric Requirements, 69 Fed. Reg. 468, 477 (interim final rule, Jan. 5, 2004) (supplementary information).

tracks and monitors the processing of asylum applications.[21] To verify the identity of asylum applicants and to conduct a background check, RAPS schedules applicants for fingerprinting at an Application Support Center.[22] The fingerprints are then sent to DHS and the FBI for comparison to those stored in other databases.[23] No fingerprints are stored in RAPS.[24] Applicants' failure to submit to fingerprinting without good cause may result in dismissal of their asylum application or waiver of adjudication before an asylum officer.[25] Such failure also automatically stops the Clock Query, which would further delay applicants' procurement of Employment Authorization Documents (EAD) and thus their ability to find work.[26] Refugees and asylum seekers who refuse to provide fingerprints are further disadvantaged because EADs must contain fingerprints.[27]

Biometric information is stored in a number of databases. The Integrated Automated Fingerprint Identification System (IAFIS), established in 1999, is the largest database of fingerprints in the world and is maintained by the Federal Bureau

---

21. *See* DHS, Privacy Impact Assessment for the Refugees, Asylum, and Parole System and the Asylum Pre-Screening System 3 (Nov. 2009), http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cis_rapsapss.pdf [hereinafter RAPS PIA]. DHS offices are able to obtain information on the more than one million applicants who have applied through the system. *Id*.

22. *See* U.S. Citizenship and Immigration Services (USCIS), Affirmative Procedures Manual 9 (2007), http://www.uscis.gov/USCIS/Humanitarian/Refugees & Asylum/Asylum/2007_AAPM.pdf [hereinafter USCIS Manual]. Applicants aged under twelve years and nine months or over seventy-five years are not required to undergo fingerprinting. *Id.* at 104. Biometric data collected includes: ten-print fingerprints captured electronically, three manually inked and digitally scanned FD-258 cards, photographs, and signatures. *See* USCIS, Privacy Impact Assessment: Biometric Storage System (BSS) 4 (2007), http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cis_bss.pdf [hereinafter BSS PIA].

23. *See* USCIS Manual, *supra* note 22, at 12–13.

24. *See* RAPS PIA, *supra* note 21, at 7.

25. *See* USCIS Manual, *supra* note 22, at 104; *see also* BSS PIA, *supra* note 22, at 14. ("USCIS benefit applications/petitions require that certain biographic information be provided and may require submission of fingerprints and photographs. . . . The failure to submit such information prohibits USCIS from processing and properly adjudicating the application/petition and thus precludes the applicant from receiving the benefit.").

26. USCIS Manual, *supra* note 22, at app. 20, 25. Asylum seekers not otherwise entitled to work in the United States must wait 180 days after the date their claim was submitted before their claim constitutes grounds for issuance of an EAD. *Id.* at 89.

27. Enhanced Border Security and Visa Entry Reform Act of 2002, Pub. Law No. 107-173, § 309 (2002).

of Investigation (FBI).[28] DHS maintains the Automatic Biometric Identification System (IDENT), which is a database of biometric information that is used for various DHS functions, including the enforcement of immigration laws.[29] Information stored in IDENT may be collected by organizations within DHS, such as US-VISIT, and by agencies external to DHS.[30] Fingerprints recorded by Application Support Centers are held in the Biometric Storage System (BSS), the repository of all USCIS biometrics.[31] Post-September 11 legislation and inter-departmental cooperation have made IDENT and IAFIS significantly interoperable; both are now searchable by officers at over 150 ports of entry.[32] BSS also interfaces with IAFIS and IDENT and is notified if its fingerprints appear in either database.[33]

2. European Union

The European Union has made extensive use of biometrics in implementing its common asylum policies. Eurodac is the EU's common fingerprinting and data comparison system. It has been described by the European Commission as "essential in ensuring the efficiency of the European Asylum System."[34] Eurodac

28. Federal Bureau of Investigation, *Integrated Automated Fingerprint Identification System or IAFIS*, http://www.fbi.gov/hq/cjisd/iafis.htm (last visited Feb. 6, 2011). *See generally* Tien-Li Loke Walsh & Bernard P. Wolfsdorf, Consular Processing in 2009—The New Electronic Era, 1768 PLI/Corp 177, 203–04 (2009) (surveying the "rapid and systemic" change in consular processing since 2001).

29. IDENT PIA, *supra* note 18, at 2.

30. *Id.* at 3. IDENT is sometimes referred to as US-VISIT/IDENT.

31. BSS PIA, *supra* note 22, at 2. BSS stores data for seventy-five years after a recorded action. *Id.* at 8.

32. *See* DHS, IDENT/IAFIS Interoperability 2–3 (May 2005), http://www.dhs.gov/xlibrary/assets/foia/US-VISIT_IDENT-IAFISReport.pdf. In order to improve accuracy and further increase compatibility with existing biometric databases, US-VISIT recently moved from collecting two fingerprints from each individual to ten fingerprints. *See* Loke Walsh & Wolfsdorf, *supra* note 28, at 193 (providing a more detailed description of cooperation between DHS and the FBI).

33. BSS PIA, *supra* note 22, at 2–3.

34. *Commission Communication to the Council and the European Parliament on Improved Effectiveness, Enhanced Interoperability and Synergies among European Databases in the Area of Justice and Home Affairs*, at 4, COM (2005) 597 final (Nov. 24, 2005). In 2006, the Commission reviewed the performance of the Central Unit of Eurodac and found it "very satisfactory . . . in terms of speed, output, security and cost-effectiveness." *Commission Staff*

was established with the aim of identifying asylum seekers who have entered the territory of its Member States unlawfully or have previously lodged asylum applications in more than one Member State.[35] It is comprised of a central database, operated by a central unit within the European Commission, which stores fingerprints submitted by Member States[36] through a streamlined procedure.[37] The directive establishing Eurodac requires Member States to collect and "promptly transmit" fingerprints of all persons seeking asylum aged at least fourteen years, but it leaves the methods by which the fingerprints are gathered to internal law, unless otherwise provided in other international and regional law.[38] Submitted fingerprints are automatically matched against the database and are retained for ten years from the date on which they were taken,[39] unless an applicant acquires citizenship, receives a residence permit, or leaves the EU at an earlier date.[40] Efforts are being made to increase Eurodac's interoperability with other biometric databases,[41] including the

---

Working Document, Annual Report to the Council and the European Parliament on the Activities of the EURODAC Central Unit in 2006, at 12, SEC (2007) 1184 (Sep. 11, 2007). The Commission reported that roughly 17% of asylum applications (or 28,593 of 165,958 cases) were subsequent applications. *Id.* at 9.

35. Council Regulation 2725/2000, Concerning the Establishment of 'Eurodac' for the Comparison of Fingerprints for the Effective Application of the Dublin Convention, 2000 O.J. (L 316) 1, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:316:0001:0010:EN:PDF [hereinafter Eurodac Regulation].

36. The Eurodac Regulation also applies in Switzerland. Council Decision 2008/147/EC, On the Conclusion on Behalf of the European Community of the Agreement between the European Community and the Swiss Confederation Concerning the Criteria and Mechanisms for Establishing the State Responsible for Examining a Request for Asylum Lodged in a Member State or in Switzerland, 2008 O.J. (L 53) 1.

37. Eurodac Regulation, *supra* note 35, at 3.

38. *Id.* at 4.

39. *Id.*

40. *Id.* at 5.

41. *See Commission Proposal for a Regulation of the European Parliament and of the Council concerning the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EC) No […/…] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person]*, at 4, COM (2009) 342 final (Sept. 10, 2009). The European Commission defines "interoperability" as the ability of IT systems and of the business processes to exchange data and to enable the sharing of information and knowledge. *See* Eurodac Regulation, *supra* note 35, at 4.

developmental Schengen Information System,[42] the Visa Information System,[43] and Europol Information System.[44]

Eurodac works synergistically with the Dublin II Regulation; together they constitute the "Dublin system,"[45] which establishes a hierarchy of criteria to determine which state is responsible for hearing an asylum claim.[46] The Regulation is intended to prevent "asylum shopping," the practice of filing multiple asylum claims in different countries, and "to ensure that each asylum applicant's case is processed by only one Member State."[47] The Regulation applies to

42. The Schengen Information System II (SIS II) improves upon its predecessor, the Schengen Information System, and allows Member States of the European Union to exchange information more easily and thereby "cooperate in implementing the various policies required in order to establish an area without internal frontiers." *See* Communication from the Commission to the Council and the European Parliament, Development of the Schengen Information System II, at 5, COM (2001) 720 final (Dec. 12, 2001).

43. The Visa Information System (VIS) improves the administration of the common visa policy and aims to prevent fraud and visa shopping, increase internal security, and facilitate the detection of persons in violation of immigration laws. *See generally* Council Regulation 767/2008, Concerning the Visa Information System (VIS) and the Exchange of Data between Member States on Short-Stay Visas (VIS Regulation), 2008 O.J. (L 218) 60 (EC) (defining the "purpose, the functionalities and the responsibilities" of the VIS).

44. The Europol Information System is used "to store, modify and utilise data that are necessary for the performance of Europol's tasks," which includes the facilitation of various levels of cooperation between national law enforcement agencies for the purpose of combating crime. EUROPA, *Europol: European Police Office*, http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l14005b_en.htm (last visited Feb. 24, 2010).

45. *Commission Proposal for a Regulation of the European Parliament and of the Council Establishing the Criteria and Mechanisms for Determining the Member State Responsible for Examining an Application for International Protection Lodged in One of the Member States by a Third-Country National or a Stateless Person*, at 2, COM (2008) 820 final (Dec. 3, 2008) [hereinafter *Commission Proposal*].

46. *See* Council Regulation 343/2003, Establishing the Criteria and Mechanisms for Determining the Member State Responsible for Examining an Asylum Application Lodged in One of the Member States by a Third-Country National, 2003 O.J. (L 50) (EC) [hereinafter Dublin II Regulation]. For example, the presence of a family member, who has been allowed to reside as a refugee in a Member State, ranks as the highest criterion for requiring that the particular Member State be responsible for examining the application of an adult asylum seeker. *Id.* at 4.

47. EUROPA, Dublin II Regulation [Legislation Summary], June 24, 2009, *available at* http://europa.eu/legislation_summaries/justice_freedom_security/free_movement_of_persons_asylum_immigration/l33153_en.htm (last visited Feb. 26, 2011). It is important to note that regulations "do not have to be

"any third country national who applies at the border or in their territory to any one of them for asylum."[48] It is binding upon all Member States, except Denmark, and it has been made applicable through agreement in Iceland and Norway.[49]

The European Commission estimates that approximately 261,000 asylum applications were lodged in the EU in 2009,[50] which represents a substantial proportion of claims filed worldwide.[51] The Commission notes that "[t]he distribution of applications across the EU suggests that the choice of the destination is not made at random but relies on several factors," which include "historical ties between countries of origin and destination, . . . the presence of established ethnic communities, and the economic situation of the countries."[52] Based on consideration of such factors, refugees might have good reasons to seek asylum in more than one Member State. However, the prevailing view is that the practice of lodging multiple applications is tantamount to "fraud and abuse," which forces national authorities to "wast[e] time on examining false asylum applications."[53] When a Eurodac fingerprint comparison reveals that

---

transposed into national law but confer rights or impose duties on the Community citizen in the same way as national law." Klaus-Dieter Borchardt, Directorate-General for Education and Culture, European Commission, The ABC of Community Law 65 (5th ed., 1999), *available at* http://ec.europa.eu/publications/booklets/eu_documentation/02/txt_en.pdf [hereinafter Borchardt, Community Law].

48. Dublin II Regulation, *supra* note 46, at 3.

49. European Council on Refugees and Exiles, *Report on the Application of the Dublin II Regulation in Europe*, AD3/3/2006/EXT/MH, 2006, at 10, *available at* http://www.unhcr.org/refworld/docid/47fdfacdd.htm [hereinafter *ECRE Report*].

50. Alberto Albertinelli, Eurostat, European Commission, Around 261,000 Asylum Applicants from 151 Different Countries were Registered in the EU-27 in 2009: Characteristics of Asylum Seekers in Europe (June 14, 2010), *available at* http://epp.eurostat.ec.europa.eu/cache/ITY_OFFPUB/KS-SF-10-027/EN/KS-SF-10-027-EN.PDF.

51. *Id.* at 2 ("Global statistics from UNHCR indicate that 922,500 asylum claims were registered in the world in 2009. . . .").

52. *Id.* Other factors, including "the perceived likelihood that the destination country will grant a protection status or the benefits connected to a protection status in the country of destination, are specific to asylum seekers." *Id.* at 3.

53. *See* Franco Frattini, *European Commissioner Responsible for Justice, Freedom and Security, Address at the Ministerial Conference on the Challenges of the EU External Border Management: Providing Europe with the Tools to Bring its Border Management into the 21st Century* (Mar. 12, 2008), *available at* http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/08/142&format=HTML&aged=1&language=EN&guiLanguage=en. The enactment of Eurodac

an asylum seeker has lodged a claim in another Member State, and the authorities believe that the other Member State is responsible for hearing the claim, the Regulation grants the authorities discretion to request, within three months of the date the application was lodged, that the other Member State "take charge" of examining the application.[54] If the requested Member State is satisfied that it is responsible, it is obliged to examine the application.[55] Under the laws of some Member States, however, an asylum seeker who is found to have moved between Member States during the consideration of her application may be deemed to have withdrawn or abandoned her claim.[56] In such cases, the responsible Member States may refuse to examine the application.[57] UNHCR has therefore noted that the combined workings of Eurodac and the Regulation disadvantage asylum seekers, since asylum seekers are precluded from moving among Member States but other third country nationals are not.[58] UNHCR has welcomed a proposal to amend Article 18(2) of the Regulation to require that Member States "complete the examination

---

was met with considerable public outcry. *See* National Biometric Security Project, *Report on International Data Privacy Laws and Application to the Use of Biometrics in the United States,* 37–38 & n.142 (Mar. 2006) (citing a number of contemporaneous public statements opposing Eurodac, the Dublin Regulation, and the assumptions underlying them) [hereinafter *NBSP Report*].

54. Dublin II Regulation, *supra* note 46, at 6.

55. *Id.*

56. These Member States include Belgium, France, Ireland, Italy, the Netherlands, Slovenia, and Spain. *ECRE Report*, *supra* note 49, at 151.

57. *Id.*

58. UNHCR, *UNHCR Comments on the European Commission's Proposal for a Recast of the Regulation of the European Parliament and of the Council Establishing the Criteria and Mechanisms for Determining the Member State Responsible for Examining an Application for International Protection Lodged in One of the Member States by a Third Country National or a Stateless Person ("Dublin II") (COM(2008) 820, 3 December 2008) and the European Commission's Proposal for a Recast of the Regulation of the European Parliament and of the Council Concerning the Establishment of 'Eurodac' for the Comparison of Fingerprints for the Effective Application of [the Dublin II Regulation] (COM(2008) 825, 3 December 2008)*, Mar. 18, 2009, at 24, *available at* http://www.unhcr.org/refworld/docid/49c0ca922.html [hereinafter *UNHCR Comments*]. The Refugee Convention allows States Parties to restrict, to the extent deemed necessary, the movement of refugees to and from third countries, but it provides that such restrictions "shall only be applied until their status in the country is regularized or they obtain admission into another country." Convention Relating to the Status of Refugees, *adopted* July 28, 1951, art. 31, 19 U.S.T. 6259, 189 U.N.T.S. 137, 174 (entered into force Apr. 22, 1954) [hereinafter Refugee Convention].

of the application" for which they are responsible, even if asylum seekers have traveled between the Member States.[59]

UNHCR has urged the Member States of the European Union to reconsider a proposed amendment to the Dublin II Regulation that would allow Member States to "mark" applicants' Eurodac records to reflect positive grants of asylum in other Member States.[60] The amendment seeks to prevent persons granted asylum from continuing to seek asylum in other Member States. However, UNHCR contends that it ignores the actual reason behind the multiplicity of asylum claims—that asylum seekers otherwise lack freedom of movement due to the interplay of the Dublin II Regulation, Eurodac, and restrictive national laws.[61] In the absence of an agreement guaranteeing asylees the right to move between Member States, asylees "remain considerably disadvantaged by comparison with other lawfully residing third country nationals."[62] UNHCR further suggests that Eurodac and the Regulation reflect a double standard whereby Member States "effectively recognize each others' negative decisions . . . [but] do not at present recognize or agree to accord any legal rights to people granted status in other Member States."[63] As further discussed below, Eurodac and the Regulation do not operate in a legal vacuum; their effectiveness in protecting the rights of refugees and asylum seekers, while shielding Member States from perceived abuse, depends on the effectiveness of other laws and policies.

The joint operation of Eurodac and the Dublin II Regulation also increases the risk that a defective asylum process in one Member State may prevent an applicant from seeking recourse in another.[64] Nowhere is this defect better illustrated than in Greece. UNHCR has expressed concern over the quality and accessibility of Greece's asylum procedures, as well as the conditions of asylum seekers' reception in Greece.[65] With respect to quality, UNHCR found Greek asylum recognition rates "disturbingly low" with an approval

59. *UNHCR Comments*, *supra* note 58, at 13.
60. *Id.* at 24.
61. *Id.*
62. *Id.*
63. *Id.* at 25.
64. *See ECRE Report, supra* note 49, at 150–52.
65. *See* UNHCR, *UNHCR Position on the Return of Asylum-Seekers to Greece under the "Dublin Regulation*," Apr. 15, 2008*, available at* http://www.unhcr.org/refworld/docid/4805bde42.html [hereinafter *UNHCR Position*].

ratio of 146 out of 25,113 asylum claims lodged in 2007.[66] Regarding accessibility, UNHCR found that Dublin II returnees lack access to translators and legal services,[67] and are detained at disproportionate levels.[68] Depending on the nationality of the individual and the circumstances of his case, the length of detention varies from two months to four years.[69]

UNHCR subsequently advised Member States "to refrain from returning asylum-seekers to Greece under the Dublin [II] Regulation until further notice."[70] Several states have complied in some manner. On April 18, 2008, Finland announced that it would require Greece to provide written assurances that asylum seekers would be fairly processed before it would transfer them to Greece;[71] Norway now makes an individualized assessment before sending asylum seekers to Greece;[72] and Germany has suspended all transfers of unaccompanied minors, unless the transfer would result in family reunification.[73] UNHCR considers that amending the Dublin II Regulation to include a mechanism for temporarily suspending transfers would have "the significant benefit of ensuring that people are not denied their basic right to a full and fair asylum claim determination."[74] Such a mechanism is currently being considered by the European Commission.[75] In its absence, however, there is a continuing risk that biometrics will be used to facilitate the

66. *Id.* ¶ 11.

67. *Id.* ¶ 7.

68. Greek authorities lack the capacity to immediately verify the identity of Dublin returnees, leading to automatic detention for many. *Id.* Those who are not automatically detained may be held under other grounds provided under Greek law, including "submitting multiple asylum applications, previously absconding, receiving a previous refusal decision on an asylum claim and to assist in the effective deportation of the application to a third country." *ECRE Report, supra* note 49, at 162 n.85.

69. *UNHCR Position*, *supra* note 65, ¶ 15.

70. *Id.* ¶ 4.

71. Human Rights Watch, Stuck in a Revolving Door: Iraqis and Other Asylum Seekers and Migrants at the Greece/Turkey Entrance to the European Union, 25 (Nov. 2008), *available at* http://www.hrw.org/en/node/76211/section/8#_ftnref29 (citing Leigh Phillips, *Finland Halts Migrant Transfer to Greece after UN Criticism*, EU Observer, (Apr. 21, 2008, 9:29 CET), http://euobserver.com/9/26016).

72. *Norway Tightens Immigration Policy*, Royal Norwegian Embassy in Canberra (Sept. 9, 2008), http://www.norway.org.au/News_and_events/Latest-News/Immigration_Policy/.

73. *UNHCR Position*, *supra* note 65, ¶ 21 n.31.

74. *UNHCR Comments*, *supra* note 58, at 11.

75. *Id.* at 11–12.

application of national laws that inadequately protect refugees and asylum seekers and violate their fundamental rights.

The joint operation of Eurodac and the Dublin II Regulation has also led to increased incidence of detention both prior to transfer[76] and following transfer if asylum seekers are returned to states that authorize the detention of asylum seekers.[77] Although the Dublin Regulation does not discuss detention, Article 18 of the Asylum Procedures Directive contemplates detention of asylum seekers so long as they are not detained "for the sole reason" that they are applying for asylum and that "there is a possibility of speedy judicial review."[78] According to UNHCR, applicants transferred under the Regulation are detained at a higher rate than other asylum applicants.[79] The Regulation's expedited procedures may perversely incentivize detention, since Member States can seek an "urgent reply" to requests for transfer,[80] provided that the asylum seeker is held in detention.[81] UNHCR maintains that the Regulation's failure to address reception conditions for Dublin returnees has been interpreted to warrant the denial of general entitlements available to refugees and asylum seekers under the Reception Conditions Directive.[82] UNHCR supports a proposed amendment to the Dublin II Regulation which would, among other things, limit detention to only "when it proves necessary, on the basis of an individual assessment of each case" and objective criteria

76. *See ECRE Report*, *supra* note 49, at 162 (noting increased use of detention prior to transfer from Belgium, the Czech Republic, Finland, Austria, the Netherlands, the U.K., and Luxembourg).

77. *Id.* ("Detention may also be imposed upon returnees in a number of Member States including Germany, the Czech Republic, Luxembourg, Belgium and Greece.") (footnotes omitted).

78. Council Directive 2005/85/EC, Minimum Standards or Procedures in Member States for Granting and Withdrawing Refugee Status, art. 18, 2005 O.J. (L 326) 13.

79. For a survey of detention rates, see UNHCR, *The Dublin II Regulation: A UNHCR Discussion Paper*, 52 n.215 (Apr. 2006), http://www.unhcr.org/refworld/docid/4445fe344.html [hereinafter *UNHCR Discussion Paper*].

80. *See supra* notes 54–57 and accompanying text.

81. Dublin II Regulation, *supra* note 46, art. 17(2), at 6.

82. *UNHCR Discussion Paper*, *supra* note 79, at 55. The Reception Conditions Directive requires Member States to enact legislation setting minimum standards for the reception of asylum seekers, along with various other rights and entitlements. *See* Council Directive 2003/9/EC, Laying Down Minimum Standards for the Reception of Asylum Seekers, 2003 O.J. (L 31) 18.

established by law, and only "if there is a significant risk of absconding."[83]

The proposal to recast the Dublin II Regulation expresses the European Commission's desire to "ensure higher standards of protection" and "contribute to better addressing situations of particular pressure on Member States' reception facilities and asylum systems."[84] While there have been calls to replace the Dublin II Regulation,[85] the Commission's efforts to recast the Regulation may meaningfully address many of the concerns listed above and thereby contribute to the responsible application of biometrics to refugees and asylum seekers.

3. United Kingdom

The United Kingdom's extensive use of biometrics merits separate discussion, both because it illustrates how national legislation may supplement EU regulations and because it provides a useful comparison to U.S. and EU practice. The Immigration and Asylum Act of 1999 provides that fingerprints of asylum seekers and their dependents[86] may be taken at the time the claim for asylum was made.[87] Under penalty of arrest, asylum seekers may be compelled, with notice, to appear for fingerprinting.[88] If an asylum seeker refuses to comply and is consequently arrested, his or her fingerprints may be obtained by use of reasonable force.[89] These procedures, operationalized through the Immigration and Asylum

83. *UNHCR Comments*, *supra* note 58, at 18.

84. *Commission Proposal*, *supra* note 45, at 5.

85. *See generally* European Council on Refugees and Exiles, *Comments from the European Council on Refugees and Exiles on the European Commission Proposal to Recast the Dublin Regulation*, at 13 (Apr. 2009), *available at* http://www.ecre.org/files/ECRE_Response_to_Recast_Dublin_Regulation_2009.pdf (arguing that the Dublin system has "extensive detrimental effects to Member States and asylum seekers" and that "[a]n alternate system based on integration accompanied by substantial solidarity measures is the only way to ensure a fair, efficient and humane CEAS").

86. Immigration and Asylum Act, 1999, c. 33, § 141(7)(e)–(f) (Eng.), *available at* http://www.opsi.gov.uk/acts/acts1999/ukpga_19990033_en_12#pt7-pb8.

87. *Id.* § 141(8)(e).

88. *Id.* § 142.

89. *Id.* § 146(2)(b).

Fingerprint System (U.K. IAFIS),[90] markedly differ from analogues administered by the USCIS.[91]

U.K. IAFIS also expands upon a pilot program requiring the collection of fingerprints from those seeking entry from specified countries, including Sri Lanka, Djibouti, Eritrea, Tanzania, and Uganda.[92] Fingerprints collected under the Immigration and Asylum Act are stored by the Immigration Fingerprint Bureau. They are retained for no longer than ten years.[93] Fingerprints are also collected from all persons applying to obtain a U.K. visa.[94] The Nationality, Immigration and Asylum Act of 2002 authorizes the Secretary of State to register applicants' "external physical characteristics" for applications to enter or remain in the United Kingdom.[95] In addition, under the U.K. Borders Act of 2007, the Home Secretary is empowered to issue regulations requiring persons subject to immigration control to obtain a document containing biometric information.[96]

B. Biometric Requirements in Refugee Travel Documents

The increased use of biometrics could help enforce a right that UNHCR has long considered "particularly important": namely,

---

90. Biometrics Working Group (BWG), Legal Issues and Biometrics - MS05, http://www.cesg.gov.uk/policy_technologies/biometrics/ms05.shtml (last visited Feb. 3, 2011); European Civil Aviation Conference, Cairo, Egypt, Mar. 22–Apr. 2, 2004, *Biometrics*, A-10–11, FAL/12-IP/2 (Dec. 3, 2003), *available at* http://www.icao.int/icao/en/atb/meetings/2004/fal12/documentation/fal12ip002_en.pdf.

91. *See supra* Part II.A.1.

92. Home Affairs Committee, Immigration Control, Fifth Report of Session 2005–06, H.C. 775-I, ¶ 171 (U.K.), *available at* http://www.publications.parliament.uk/pa/cm200506/cmselect/cmhaff/775/775i.pdf [hereinafter Home Affairs Committee Report]. The program was enacted to address a perceived high incidence of fraudulent claims submitted by nationals of those countries. *Id.*

93. *See* Immigration and Asylum Act, § 143(1), (15).

94. Home Affairs Committee Report, *supra* note 92, at 47–48; *see also* Foreign & Commonwealth Office, Better World, Better Britain, Departmental Report, 2008, Cm. 7398, at 106 (U.K.) (reporting that finger scans were required for anyone applying for a U.K. visa beginning in January 2008).

95. Nationality, Immigration and Asylum Act, 2002, c. 41, § 126 (U.K.), *available at* http://www.opsi.gov.uk/Acts/acts2002/ukpga_20020041_en_10#pt6-pb5-l1g126; European Civil Aviation Conference, *supra* note 90, at A-10.

96. U.K. Borders Act 2007, c. 30, § 5, *available at* http://www.legislation.gov.uk/ukpga/2007/30/section/5; *see also* Home Office, U.K. Borders Bill, Regulatory Impact Assessment (2007), at 2 (describing the purpose and intended effect of the Act).

the right of refugees to travel in order to seek opportunities for education, training, and employment.[97] Refugee travel documents (RTDs) are integral in preserving refugees' freedom of movement, both within countries of refuge and in third countries, particularly when refugees have lost their travel documents or only have expired documents that they are unable to replace. Biometric identifiers have been incorporated in travel documents issued by numerous states, but refugee travel documents issued by UNHCR, which are known as Convention Travel Documents (CTDs) because they are issued pursuant to the Convention Relating to the Status of Refugees (Refugee Convention),[98] and by states lacking in technical capacity, have not kept pace. As travel-related security concerns loom ever larger, challenges to the authenticity of CTDs and outdated RTDs are becoming increasingly common, thereby undermining refugees' ability to move freely.[99] Biometrics therefore should be incorporated into CTDs, to the extent possible given UNHCR's limited mandate, and RTDs, to the extent financially and technically possible for the issuing state, with the aim of protecting refugees' rights. However, care should be taken to minimize the concerns posed by biometrics.[100]

1. Biometric Requirements in Passports and the Obsolescence of CTDs and Some RTDs

Substantial developments in biometric identification in general travel documents have helped to make CTDs and some RTDs obsolete. On May 28, 2003, the ICAO[101] announced the adoption of a

97. UNHCR, *Note on Travel Documents for Refugees*, ¶¶ 1–2, EC/SCP/10 (Aug. 30, 1978), *available at* http://www.unhcr.org/refworld/docid/3ae68cce14.html [hereinafter *UNHCR Note on RTDs*].

98. During 2005, UNHCR issued CTDs to 2,210 refugees in fourteen countries. UNHCR, *Measuring Protection By Numbers (2005)*, at 16 (Nov. 2006), *available at* http://www.unhcr.org/refworld/docid/45ba06444.html.

99. The former Immigration and Naturalization Service (INS) reported that 271 RTDs were seized in FY 1998, 1,107 in FY 1999, 153 in FY 2000, and 702 in FY 2001. *Identity Fraud: Prevalence and Links to Alien Illegal Activities: Hearing Before the Subcomm. on Crime, Terrorism and Homeland Security and the Subcomm. on Immigration, Border Security, and Claims of the H. Comm. on the Judiciary*, 107th Cong. (2002) (statement of Richard M. Stana, Dir., Justice Issues, Gen. Accounting Office).

100. *See infra* Part III.

101. The ICAO was formed pursuant to Article 43 of the Convention on International Civil Aviation. Convention on Int'l Civil Aviation art. 43, Dec. 7, 1944, 61 Stat. 1180, 15 U.N.T.S. 295 (entered into force Apr. 4, 1947). It is a specialized agency of the United Nations and is charged with, *inter alia*,

"global, harmonized blueprint for the integration of biometric identification information into passports and other Machine Readable Travel Documents (MRTDs)."[102] The ICAO decided that these travel documents, dubbed "e-Passports," will utilize facial recognition as their primary means of biometric identification, but it allowed states the option to use secondary biometrics to supplement facial recognition.[103] The information, along with biographical information and a digital photograph, would be stored in contactless RFID chips embedded within the MRTDs.[104]

National and regional action has also spurred the incorporation of biometric identifiers into MRTDs. The Enhanced Border Security and Visa Entry Reform Act of 2002 (the Border Security Act) required the U.S. Department of State and USCIS to use biometric identifiers in visas and other travel documents by October 26, 2004.[105] Since August 2007, all travel and entry documents issued by the State Department have met these specifications.[106] The Border Security Act also requires other countries to incorporate biometric identifiers that satisfy the standards of the ICAO in order to remain eligible for the Visa Waiver

---

"insur[ing] the safe and orderly growth of international civil aviation throughout the world." *Id.* art. 44. By adopting standards and issuing regulations, the ICAO facilitates cooperation among its Contracting States. It continues to organize worldwide and regional symposia on biometrics and security standards and provides operational assistance in the implementation of MRTD-related projects. *See* U.N. Secretary-General, *Measures to Eliminate International Terrorism*, ¶ 145*, delivered to the General Assembly*, U.N. Doc. A/64/161 (July 22, 2009).

102. *See* ICAO, Biometrics Announcement, *supra* note 12. MRTDs contain identification data, including, perhaps, biometric data, in a standardized format readable by other states that issue MRTDs. *See* ICAO, *MRTD Overview*, http://www2.icao.int/en/MRTD/Pages/Overview.aspx (last visited Feb. 3, 2011). By April 1, 2010, all travel documents issued by the ICAO's members were to have been machine readable, but far from all of them will contain biometric identifiers. News Release, ICAO, *Issuance Systems and Border Security the Focus of Second ICAO Symposium on Machine Readable Travel Documents*, PIO 09/06 (July 5, 2006), *available at* http://www.icao.int/icao/en/nr/2006/pio200609_e.pdf.

103. ICAO, Biometrics Announcement, *supra* note 12.

104. *See* Mike Ellis, *39 Myths about e-Passports: Part I*, 24, ICAO MRTD Report, Vol. 5, No. 1, 2010.

105. *See* Enhanced Border Security and Visa Entry Reform Act of 2002, Pub. L. No. 107-173, § 303(b)(1), 116 Stat. 543, 553 (2002) [hereinafter Border Security Act]; *see also* Loke Walsh & Wolfsdorf, *supra* note 28, at 189–90 (describing State Department and DHS implementation of visa programs incorporating biometric identifiers).

106. *The U.S. Electronic Passport*, U.S. Dep't of State, http://travel.state.gov/passport/passport_2498.html (last visited Feb. 4, 2011).

Program.[107] The Council of the European Union has promulgated a Council Regulation providing for the establishment of standard biometric features for biometrics in passports and travel documents issued by Member States.[108] By 2007, these requirements helped spur "some 40 States,"[109] including Germany,[110] South Africa,[111] Australia,[112] and Poland,[113] to incorporate biometrics into travel documents.

---

107. Border Security Act, § 303(c)(1). The deadline was initially October 26, 2004, but it was later extended to October 26, 2006. Loke Walsh & Wolfsdorf, *supra* note 28, at 194. The Visa Waiver Program (VWP) "enables eligible nationals of certain countries to travel to the United States for tourism or business for stays of 90 days or less without obtaining a visa." Press Release, Dep't of Homeland Sec., Frequently Asked Questions: Electronic System For Travel Authorization (ESTA) (June 3, 2008), *available at* http://www.dhs.gov/xnews/releases/pr_1212501117599.shtm.

108. *See* Council Regulation 2252/2004, On Standards for Security Features and Biometrics in Passports and Travel Documents Issued by Member States, 2004 O.J. (L 385) 1 (EC) (providing that passports and travel documents issued by Member States shall include a facial image and fingerprints).

109. In 2006, ICAO stated that by the next year, ePassports would be "deployed by some 40 States." 189 States have agreed to "begin issuing ICAO-standard Machine Readable Passports (MRPs)" by April 2010. News Release, ICAO, *supra* note 102.

110. Passgesetz [Passport Act], Apr. 19, 1986, BGBl. I at 537, § 4(3), *available at* http://www.unhcr.org/refworld/docid/48e5dc512.html.

111. Refugees Amendment Act 33 of 2008 § 15, *available at* http://www.unhcr.org/refworld/docid/4a54bbd4d.html.

112. *See, e.g.*, *Migration Legislation Amendment (Identification and Authentication) Act 2004*, *available at* http://www.comlaw.gov.au/Details/C2004A01237 (expanding the grounds for collecting biometric information from non-Australian citizens on entry to and departure from Australia). In October 2005, Australia adopted the "ePassport, a biometric passport using facial recognition technology introduced by DFAT [Department of Foreign Affairs and Trade] . . . ." Dean Wilson, *Australian Biometrics and Global Surveillance*, 17 Int'l Crim. Just. Rev. 207, 212 (2007). On October 25, 2005, the Minister of Foreign Affairs announced that biometrically-enabled ePassports would be issued to all new passport applicants and for passport renewals. Media Release, Australian Minister of Foreign Affairs, Australia Launches ePassports (Oct. 25, 2005), http://www.foreignminister.gov.au/releases/2005/fa132_05.html.

113. Act on Aliens, 2003, Journal of Laws of 2003, No 128, it. 1175, arts. 12(a), 14, 93, 101, *available at* http://www.unhcr.org/refworld/docid/44a133374.html (providing for fingerprinting upon entry, expulsion, or detention) [hereinafter Polish Act on Aliens].

2. Legal Framework Governing Refugee Travel Documents and the Need for Modernization

Article 27 of the Refugee Convention requires that Contracting States issue identity papers to any refugee in their territory who does not possess a valid travel document.[114] Article 28 provides that Contracting States "shall issue to refugees lawfully staying in their territory travel documents for the purpose of travel outside their territory, unless compelling reasons of national security or public order otherwise require."[115] The Schedule to the 1951 Refugee Convention further describes Contracting States' obligations in issuing and recognizing RTDs,[116] and provides a template to which travel documents issued pursuant to Article 28 must conform.[117] The Schedule, however, makes no mention of biometrics, and aside from a recommendation that it be printed in a manner that would allow detection of erasure or alteration, it lacks anti-fraud protections.[118] Furthermore, the Schedule has not been amended since its adoption in 1951.

Due to the silence of the Convention and its Schedule, there is considerable variation among RTDs in their incorporation of biometrics and, consequently, their resistance to fraud. Some are quite sophisticated, such as those issued in the United States pursuant to the Immigration and Nationality Act, and incorporate

---

114. Refugee Convention, *supra* note 58, art. 27. *See generally* United Nations Treaty Collection, *available at* http://treaties.un.org/Pages/ViewDetailsII.aspx?&src=TREATY&mtdsg_no=V~2&chapter=5&Temp=mtdsg2&lang=en (last visited Feb. 27, 2010) (listing 144 States Parties to the Refugee Convention, including the United States).

115. Refugee Convention, *supra* note 58, art. 28.

116. *Id.* Contracting States must issue RTDs (1) for the purpose of travel, and (2) to refugees lawfully staying in their territory. A Contracting State cannot refuse to issue RTDs because it disapproves of refugees' reasons for traveling. The second element is supplemented by Article 28, which allows Contracting States discretion to issue RTDs to any refugee within their territory. *UNHCR Note on RTDs*, *supra* note 97, ¶¶ 13–15. The Schedule to the Convention requires that RTDs be valid for either one or two years. *See, e.g.*, Polish Act on Aliens, *supra* note 113, art. 73. ("[T]he Polish travel document for an alien shall be valid for the period not exceeding 2 years."); U.S. RTDs are also generally valid for two years. USCIS, Instructions for Form I-131, Application for Travel Document 2, http://www.uscis.gov/files/form/i-131instr.pdf.

117. *See* Refugee Convention, *supra* note 58. UNHCR has urged States to follow the template, and because the majority of States have done so, RTDs are more immediately recognizable to immigration officials. *UNHCR Note on RTDs*, *supra* note 97, ¶ 11.

118. *UNHCR Note on RTDs*, *supra* note 97, ¶¶ 40–47.

biometric identifiers.[119] Indeed, recently revised USCIS instructions require applicants for refugee travel documents to provide fingerprints at an Application Support Center.[120] In contrast, CTDs issued by UNHCR do not incorporate biometric identifiers. CTDs are issued when states lack the financial or technical capacity to issue RTDs, and they are the equivalent of RTDs, except that their holders are not entitled to the consular protection typically afforded by states.[121] UNHCR has recognized that CTDs require modernization, and in late September 2009, the Assistant High Commissioner for Protection, Erika Feller, said in a statement:

> The problem is that this model was drawn up in an earlier age, before such innovations as machine-readable passports and biometric inclusions in travel documents. There is now an urgent need for new formats, compatible with ever more stringent country requirements, if the CTD is to be accepted as a legitimate document for travel.[122]

3. Updating Convention Travel Documents

Although it is not entirely clear whether UNHCR can update the CTDs without a concurrent revision of the Refugee Convention and its Schedule, there are solid grounds for interpreting the Refugee Convention to allow improvement of the CTDs. Article 31(3)(b) of the Vienna Convention on the Law of Treaties (Vienna Convention) provides that "any subsequent practice in the application of the

---

119. 8 U.S.C. §§ 1181–1182 (2006). For more detailed requirements, see 8 C.F.R. § 223 (1998). *See generally* Taiga Takahashi, Note, *Left Out at Sea: Highly Migratory Fish and the Endangered Species Act*, 99 Calif. L. Rev. 179, 216 (2011) (discussing divergent state implementations of international agreements relating to environmental protection, which also create a "floor of protection" but do not preclude Member States from regulating more strictly).

120. *See* USCIS, *USCIS Biometric Changes for Re-Entry Permits and Refugee Travel Documents*, Mar. 5, 2008, http://www.uscis.gov/files/article/i-131_biometrics_uscisupdate_03052008.pdf; *see also* USCIS, Instructions for Form I-131, Application for Travel Document, at 5. The revised instructions only cover applicants aged 14 through 79, *id.*, and require such applicants to pay an additional, non-waivable $80 biometric fee, raising the total filing fee to $385. *Id.* at 8.

121. *See UNHCR Note on RTDs*, *supra* note 97, ¶ 2.

122. UNHCR, Statement of Ms. Erika Feller, *Assistant High Commissioner—Protection, at the Sixtieth Session of the Executive Committee of the High Commissioner's Programme* 6–7 (Sept. 30, 2009), http://www.unhcr.org/refworld/docid/4ac4ac772.html.

treaty which establishes the agreement of the parties regarding its interpretation" shall be taken into account.[123] The sustained efforts of the ICAO and its member states in issuing machine-readable travel documents containing biometric identifiers, both to regular travelers and refugees, should place the issuance of updated, biometric CTDs within the ambit of the Refugee Convention and its Schedule.

Article 31(1) of the Vienna Convention further states: "A treaty shall be interpreted in good faith in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in the light of its object and purpose."[124] The Refugee Convention provides that one of its goals is "to revise and consolidate previous international agreements relating to the status of refugees and to extend the scope of and protection accorded by such instruments."[125] The issuance of RTDs predates the 1951 Refugee Convention and was the subject of the first international agreement reached for the express benefit of refugees.[126] These early travel documents, known as "Nansen Passports," constituted a single sheet of paper and therefore did not resemble national passports, thereby decreasing their durability and recognizability.[127] Some Nansen Passports also failed to indicate the duration of their validity.[128] These deficiencies were remedied by the Inter-Governmental Agreement on Refugee Travel Documents, which was signed in London on October 15, 1946 and contained provisions similar to the 1951 Refugee Convention.[129] Therefore, given that RTDs had been used and updated for decades before the adoption of the Refugee Convention, and given that an aim of the Refugee Convention is to increase protection afforded to refugees, the Convention's silence with respect to biometrics should not be

123. Vienna Convention on the Law of Treaties, *opened for signature* May 23, 1969, art. 31, 1155 U.N.T.S. 331, 340 (entered into force Jan. 27, 1980).

124. *Id.*

125. Refugee Convention, *supra* note 58, pmbl.

126. *UNHCR Note on RTDs*, *supra* note 97, ¶ 6.

127. *Id.*

128. *Id.*

129. Final Act of the Intergovernmental Conference on the Adoption of a Travel Document for Refugees and Agreement Relating to the Issue of a Travel Document to Refugees Who Are the Concern of the Intergovernmental Committee on Refugees, Oct. 15, 1946, 11 U.N.T.S. 150. *See also* International Refugee Organization, *Memorandum Submitted by the Representative of the International Refugee Organisation*, E/AC.32/L.39, Feb. 19, 1950, http://www.unhcr.org/refworld/pdfid/40aa12354.pdf (listing the parties to the London Agreement, along with their actions taken pursuant to the agreement, as of Oct. 4, 1949).

interpreted to preclude their use. It makes eminent sense for UNHCR to emulate the best practices of states and thereby contribute to improving security while protecting refugees' freedom of movement.

Against the above points, it could be argued that the Refugee Convention should be interpreted to mandate UNHCR fidelity to its prescriptions of the content and form of RTDs. Although the Convention makes no mention of biometrics, it does devote significant attention to describing the content, legal significance, and format of the travel documents.[130] The drafters of the Convention were surely aware of the need to make RTDs resistant to fraud, since its annexed template recommends that the RTDs be printed in a manner that would facilitate the detection of erasure or alteration.[131] Furthermore, the drafters must have been well aware of fingerprinting, which had been in use for quite some time.[132] While there might be some truth to these arguments, the operation of the Vienna Convention, as described above, favors a permissive reading of the Refugee Convention.

C. Biometrics in Refugee Camps and Entitlement Programs

While the more typical uses of biometrics described above have been subject to criticism by supporters of refugee rights,[133] UNHCR has successfully used biometrics in refugee camps to assist in the registration of refugees and to prevent errors and fraud.

---

130. *See* Refugee Convention, *supra* note 58, Schedule.

131. *Id.*, Specimen Travel Document.

132. A colorful article written in 1885 reports that fingerprint identification was used by a police constable in Albany, New York to identify a burglar who "broke a pane of glass . . . and accidentally left an impression of his blood-besmeared thumb on a piece of paper." *Thumbs down! The Latest Plan for Outwitting the Chinese: Thumbmarks for Identification*, S.F. Daily Report, Sept. 19, 1885, at 8. The exact date of this incident is unknown but has been estimated to have occurred "[s]ometime in the late 1850s." Simon A. Cole, Suspect Identities: A History of Fingerprinting and Criminal Identification 121 (2001) [hereinafter Cole, Suspect Identities] (arguing that "fingerprint identification in the Americas was stimulated by a perceived need to identify 'faceless,' facially unfamiliar 'hordes' of people who came in successive waves to their shores"). For a better documented example, see Scientific Working Group on Friction Ridge Analysis, Study and Technology (SWGFAST), et al., The Fingerprint Sourcebook 1–12 (2009), http://www.ojp.usdoj.gov/nij/pubs-sum/225320.htm (noting that the New York Civil Service Commission made systematic use of fingerprints as early as 1902). All criminals in New York were subject to fingerprinting in 1903. *Id.*

133. *See infra* Part III.

UNHCR is expanding its capacity to make use of biometrics, and the refugees under its protection will likely benefit as a result. Fraud may occur when individuals attempt to register multiple times under different names in order to obtain more than their share of aid.[134] Fraud inflates the population of refugee camps, strains their resources, and contributes to an inequitable distribution of goods and services. The use of biometrics has proven to be an effective check. For example, their use in the registration of refugees in the Ali Addeh refugee camp in Djibouti helped reveal that the population had been overestimated by some four thousand individuals.[135] In 2007, UNHCR conducted its largest registration exercise in Pakistan in collaboration with the Pakistani Government.[136] By February 15, 2008, more than two million Afghan refugees were registered and had received "Proof of Registration" cards containing biometric data, specifically facial recognition and fingerprints.[137]

The use of biometrics for the identification and documentation of refugees and asylum seekers finds support in the conclusions of the governing body of UNHCR, the Executive

134. *See generally* UNHCR, UNHCR Global Report 2006, Pakistan (June 2007), http://www.unhcr.org/refworld/docid/466d3fb62.html [hereinafter *UNHCR Global Report*] (reporting on UNHCR's efforts to support Afghan refugees and asylum-seekers in Pakistan in such areas as community services, domestic needs and household support, education, health and nutrition, legal assistance, operational support for agencies, sanitation, shelter and infrastructure, transport and logistics, and water). To the consternation of many, biometrics have also been applied, albeit infrequently, to prevent fraud among recipients of public assistance in the United States. For example, food stamp recipients in New York City, Arizona, Texas, and California are required to submit to fingerprinting. Kaomi Goetz, *Fingerprinting for Food Stamps under Scrutiny,* National Public Radio, Dec. 18, 2009, http://www.npr.org/templates/story/story.php?storyId=121560340.

135. United States Agency for International Development (USAID), Visit to a Refugee Camp in Djibouti, Mar. 2, 2007, http://eastafrica.usaid.gov/en/Article.1053.aspx.

136. *See generally* UNHCR Global Report, *supra* note 134 (noting that UNHCR registered 2.15 million Afghan refugees living in Pakistan).

137. UNHCR, UNHCR Country Operations Plan 2008: Pakistan 3 (Sept. 1, 2007), http://www.unhcr.org/refworld/docid/46f7d5f32.html. Afghans over the age of five received their own Proof of Registration cards, while children under five were listed on their mothers' cards. *Id.* The cards are to remain valid for three years and allow Afghan refugees to remain in Pakistan for the duration of their validity. *Id.* at 5. UNHCR meanwhile continues to assist refugees who seek repatriation to Afghanistan. *Id.*

Committee of the High Commissioner's Programme (ExCom).[138] The conclusions, rendered in 2001 and 2005, also encourage states and UNHCR to develop a standardized worldwide registration system.[139] UNHCR's commitment to the development of biometric identification and documentation is further reflected in the Agenda for Protection, which is a plan to improve the international protection regime for refugees and asylum seekers.[140] The Agenda has been endorsed by ExCom, welcomed by the United Nations General Assembly, and purports to reflect the "broad consensus on what specific actions can and should be undertaken to achieve certain agreed goals in refugee protection."[141]

UNHCR launched Project PROFILE in order to implement the ExCom Conclusions relevant to biometrics. Among the general aims of PROFILE is increasing UNHCR's ability to identify the size and nature of refugee populations and to collect and analyze such information more effectively.[142] In furthering this aim, PROFILE envisioned the continued development of worldwide data management software, the introduction of an automatic fingerprint information system, and the issuance of identity documents containing fingerprint data.[143]

UNHCR added a biometric fingerprint module to its registration tool in five country operations by 2007.[144] This expansion

---

138. The two most relevant conclusions are No. 91 (LII) and No. 102 (LVI). Conclusion No. 91 (LII) "*encourages* States and UNHCR to introduce new techniques and tools to enhance the identification and documentation of refugees and asylum-seekers, including biometrics features, and to share these with a view towards developing a more standardized worldwide registration system." UNHCR, Thematic Compilation of Executive Committee Conclusions 153 (4th ed. 2009), *available at* http://www.unhcr.org/refworld/docid/4a7c4b882.html. Conclusion No. 102 (LVI) "*encourages* further progress in introducing new techniques and tools, including biometrics features." *Id.* at 149.

139. *Id.* at 153.

140. UNHCR, Agenda for Protection 40 (3rd ed. 2003), *available at* http://www.unhcr.org/refworld/docid/4714a1bf2.html.

141. *Id.* at 5, 9.

142. UNHCR, Resettlement Handbook IX/3 (2004), *available at* http://www.unhcr.org/refworld/docid/3ae6b35e0.html.

143. *Id.*

144. UNHCR, *Note on International Protection: Report by the High Commissioner* 4, U.N. Doc. A/AC.96/1038 (June 29, 2007), *available at* http://www.unhcr.org/refworld/docid/469377852.html. The module supplements "proGres," the UNHCR registration tool created under Project PROFILE. *Id.* As of 2007, proGres had been used in 51 countries and held contained records on more than 2.5 million persons of concern to UNHCR. *Id.*

of biometric capacity occurred partially in response to concerns raised by UNHCR staff in the Dadaab and Kakuma refugee camps in Kenya.[145] Because Somali refugees are granted *prima facie* refugee status, it was believed that some Kenyan nationals were entering the camps and claiming to be from Somalia.[146] It was further believed that existing registration software was ineffective in detecting persons registering under different names in order to obtain additional goods and services. The UNHCR *Handbook for Registration* was consequently revised and now provides that "[v]erification to prevent multiple registration can involve a routine check of the registration database . . . and, if possible/available, photographs or biometric data."[147]

UNHCR now registers and obtains fingerprints from new arrivals before making certain entitlements available to refugees in the Dadaab and Kakuma camps.[148] UNHCR also coordinates with the Kenyan government by cross referencing fingerprints of individuals aged fifteen and older with the Kenyan biometric database, and it is thereby able to avoid registering of Kenyan nationals attempting to obtain assistance in the camps.[149] These efforts help ensure that scarce international aid is directed towards those who have lost their homes, livelihoods, and loved ones in Sudan and Somalia.

---

145. UNHCR, Analysis of Refugee Protection Capacity: Kenya 19 (Apr. 2005), http://www.unhcr.org/refworld/docid/472896f70.html.

146. Human Rights Watch, From Horror to Hopelessness: Kenya's Forgotten Somali Refugee Crisis 17 (Mar. 30, 2009), *available at* http://www.unhcr.org/refworld/docid/49d092872.html [hereinafter HRW, From Horror to Hopelessness].

147. UNHCR, UNHCR Handbook for Registration 86 (2003), *available at* http://www.unhcr.org/refworld/docid/3f967dc14.html [hereinafter UNHCR Handbook for Registration].

148. HRW, From Horror to Hopelessness, *supra* note 146, at 35.

149. Immigration and Refugee Board of Canada, Somalia: Documentation and Other Means of Identification of Somalis in United Nations High Commissioner for Refugees (UNHCR) Camps in Djibouti, Egypt, Ethiopia, Kenya and Yemen, SOM102473.E (May 4, 2007), http://www.unhcr.org/refworld/docid/47d6547723.html. In 2006, registration of Somali refugees in Kenya was temporarily suspended to allow the Kenyan government to fingerprint those who had recently lodged asylum claims. *See* UNHCR, *Registration of Somali Refugees in Kenya Resumes* (Nov. 3, 2006), http://www.unhcr.org/news/NEWS/454b22e12.html.

D. Biometric Identification as a Means of Reducing the Incidence of Detention

The registration of the biometric characteristics of refugees and asylum seekers and the issuance of documentation containing biometric identifiers has effectively been used to lower their incidence of detention by national authorities.[150] Refugees in Zambia must obtain permission from the national Commissioner for Refugees in order to reside outside of refugee camps.[151] Those refugees who obtain permission are issued electronic identity cards, which contain biometric data that is backed up onto a central database.[152] This reduces the likelihood that refugees will be erroneously returned to the camps if their identity cards are lost or stolen, thereby improving refugees' security.[153]At the same time, the Government of Zambia is assured that the benefits it grants to some refugees are not stolen and misused by others. A research paper commissioned by UNHCR endorsed the program as a "clear demonstration that the regularisation/registration of urban refugees, using an effective electronic system, can reduce the incidence of detention."[154]

---

150. *See generally* UNHCR, Alternatives to Detention of Asylum Seekers and Refugees, UNHCR Doc. POLAS/2006/03 (Apr. 2006), http://www.unhcr.org/refworld/docid/4472e8b84.html [hereinafter UNHCR, Alternatives to Detention] (suggesting that alternatives to detention of refugees may be more efficient and are more cost-effective but rarely used). Personal liberty is protected by a number of instruments in international law, including the Universal Declaration of Human Rights, G.A. Res. 217A, at 73, U.N. GAOR, 3d Sess., art. 9, U.N. Doc. A/810 (Dec. 12, 1948) [hereinafter UDHR]; the International Covenant on Civil and Political Rights, *opened for signature* Dec. 16, 1966, art. 9, S. Exec. Doc. E, 95-2 (1978), 999 U.N.T.S. 171, 175 (entered into force Mar. 23, 1976) [hereinafter ICCPR]; the American Convention on Human Rights, *opened for signature* Nov. 22, 1969, art. 7, O.A.S.T.S. No. 36, 1144 U.N.T.S. 123, 147 (entered into force July 18, 1978); the Convention on the Rights of the Child, *opened for signature* Nov. 20, 1989, art. 37(b), 1577 U.N.T.S. 3, 55 (entered into force Sept. 2, 1990) [hereinafter Children's Convention]; and the International Convention on the Protection and Promotion of the Rights and Dignity of Persons with Disabilities, art. 14, Dec. 13, 2006, 46 I.L.M. 443 (entered into force May 3, 2008).

151. UNHCR, Alternatives to Detention, *supra* note 150, at 253.

152. *Id.* at 255.

153. According to Mohamed Mahdi, a Somali refugee in Djibouti: "The ID card is very important for us. It is good for our own safety. I am not a Djiboutian citizen and when I go to town, I could be arrested by the police, just for being a refugee and not having an ID. This ID card will help protect me from being arrested." UNHCR, *Djibouti: Refugees Grasp Security in their Hands with New ID Cards* (Aug. 25, 2009), http://www.unhcr.org/4a93b6166.html.

154. UNHCR, Alternatives to Detention, *supra* note 150, at 255.

Biometrics improve the effectiveness of such systems by simultaneously reducing the system's susceptibility to fraud, since biometric characteristics are largely immutable,[155] and allowing refugees who lack documentation to credibly establish their identity.

The implementation of biometrics by European authorities suggests that biometrics can be used to either prevent or aid in the detention of refugees and asylum seekers, depending on the policies of the state. In order to reduce the risk of wrongful arrest, Bulgaria's State Agency for Refugees issues identity documents to asylum seekers one day after their registration.[156] The incidence of detention in Denmark is relatively low, and the implementation of alternatives to detention, such as posting bail or reporting to the police at specified intervals, is facilitated by the registration of asylum seekers' fingerprints at reception centers.[157] The fingerprints of asylum seekers in Germany, however, are used in connection with their accommodation in typically isolated collective centers for the duration of their application.[158]

III. PRIVACY INTERESTS AND OTHER CONCERNS

This part addresses whether the collection and retention of biometric information interferes with refugees' and asylum seekers' privacy interests. Part III.A provides a brief overview of the legal instruments which protect privacy interests. Part III.B assesses whether the collection of biometrics, specifically fingerprinting,[159] undermines refugees' and asylum seekers' privacy interests. With respect to the United States, it argues that fingerprinting refugees and asylum seekers would not likely constitute a search under the Fourth Amendment. At the same time, it suggests that scientific developments may give the Supreme Court reason to hold that fingerprinting is a search, owing to the possibility that fingerprints may reveal personal and medical information. However, even assuming that it does, fingerprinting refugees at national borders and ports of entry would not be unreasonable, as it would likely fall under the border search exceptions to the general requirement that

155. *See supra* notes 8–10 and accompanying text.
156. UNHCR, Alternatives to Detention, *supra* note 150, at 35.
157. *Id.* at 96–97.
158. *Id.* at 111.
159. The focus on fingerprinting is warranted because fingerprinting is the most commonly used biometric modality and most frequently affects refugees and asylum seekers. *See supra* note 11 and accompanying text.

searches be authorized by warrants based upon probable cause. However, conditioning the applications of asylum seekers upon their willingness to undergo fingerprinting is more problematic, since it is unlikely that persons fleeing from a well-founded fear of persecution give voluntary consent. Although EU law recognizes a fundamental right to privacy with respect to the processing of personal data, it contains consent and "public interest" exceptions and thereby provides Member States ample grounds to collect biometric information.[160]

Part III.C then addresses how the retention of biometric information affects refugees' and asylum seekers' privacy interests, drawing upon both U.S. and European law. First, it suggests implementing measures to restrict the transfer of information stored in biometric databases. Second, it argues that the retention period for refugees' and asylum seekers' biometric information should be shortened, since the current U.S. practice of storing data long-term threatens refugees' and asylum seekers' privacy and security. The remainder of this part discusses other concerns: namely, the threat of misidentification and the potential reluctance of refugees and asylum seekers to undergo fingerprinting.

It should be recognized at the outset that refugees and asylum seekers are likely to consider biometric enrollment, such as fingerprinting, to be a more serious intrusion than those who have not shared their experiences. Refugees and asylum seekers either face, have faced, or have a well-founded fear of facing persecution by the government or persons whom the government is unable or unwilling to control.[161] As such, their reluctance to disclose their

160. Council and Parliament Directive 95/46/EC, On the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1981 O.J. (L 281) 31 (EC), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML [hereinafter EU Privacy Directive].

161. 8 U.S.C. § 1101(a)(42)(A) (2006) (defining "refugee" as any person who cannot return to, and who "is unable or unwilling to avail himself or herself of the protection of, [her home] country because of persecution or a well-founded fear of persecution on account of race, religion, nationality, membership in a particular social group, or political opinion"); *see also* Refugee Convention, *supra* note 58, art. 1(a)(2) (defining refugee as any person who "owing to well-founded fear of being persecuted for reasons of race, religion, nationality, membership of a particular social group or political opinion, is outside the country of his nationality and is unable or, owing to such fear, is unwilling to avail himself of the protection of that country; or who, not having a nationality and being outside

largely immutable biometric identity should merit special consideration. While these reservations may be less pronounced when admission or entitlements are sought from a particular state, since in such cases it would seem reasonable to require refugees and asylum seekers to provide some personal information in return, refugees and asylum seekers lack assurances that their biometric information will not be shared with third countries, which could potentially undermine their safety.[162] Finally, given the well-documented hostility towards asylum seekers within some circles,[163] refugees and asylum seekers are more likely to consider fingerprinting to be a badge of criminality.[164]

A. Sources of Protection

Privacy interests find protection under the Fourth and Fourteenth Amendments to the U.S. Constitution,[165] state constitutional analogues,[166] and a number of federal and state statutes and regulations, including the Privacy Act of 1974.[167] Relevant international instruments include the Universal Declaration of Human Rights,[168] the International Covenant on Civil

---

the country of his former habitual residence as a result of such events, is unable or, owing to such fear, is unwilling to return to it").

162. *See infra* notes 227–228 and accompanying text. *See also* European Council on Refugees and Exiles, Defending Refugees' Access to Protection in Europe 33–34 (2007), *available at* http://www.unhcr.org/refworld/docid/4766464e2.html [hereinafter ECRE, Defending Refugees' Access] (stating that the broad definition of availability of information poses the threat of violation of right to privacy and that there should be a guarantee that sensitive information will not be shared with third countries that can result in the detriment of one's safety).

163. *See, e.g.*, European Comm'n against Racism and Intolerance, *Annual Report on ECRI's Activities* 10 (2009), *available at* http://www.coe.int/t/dghl/monitoring/ecri/activities/Annual_Reports/Annual%20report%202008.pdf (noting that migrants, refugees and asylum seekers are "particularly subject to the negative climate of opinion" and are "too often presented as the persons responsible for the deterioration of security conditions, unemployment and increased public expenditure").

164. *See infra* notes 254–272 and accompanying text.

165. *See* Roe v. Wade, 410 U.S. 113, 152–53 (1973).

166. *See* Privacy Protections in State Constitutions, http://www.ncsl.org/default.aspx?tabid=13467 (last visited Feb. 10, 2011) (explaining that constitutions in ten states expressly recognize the right to privacy, while the highest courts of other states have established constitutional privacy rights).

167. 5 U.S.C. § 552a (2006).

168. Article 12 provides: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour

and Political Rights,[169] and the U.N. General Assembly's Guidelines on Computerized Data Files.[170] Numerous regional instruments are relevant, including: the European Convention on Human Rights,[171] the Charter of Fundamental Rights of the European Union,[172] the Convention on Human Rights and Biomedicine,[173] the Data Protection Convention, [174] and directives of the European Parliament.[175]

---

and reputation. Everyone has the right to the protection of the law against such interference or attacks." UDHR, *supra* note 150, art. 12.

169. Article 17(1) states: "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, or correspondence, nor to unlawful attacks on his honour and reputation." ICCPR, *supra* note 150, art. 17(1). Article 17(2) further provides: "Everyone has the right to the protection of the law against such interference or attacks." *Id.*

170. Guidelines for the Regulation of Computerized Personal Data Files, G.A. Res. 45/95, ¶ 1, U.N. Doc. A/RES/45/95 (Dec. 14, 1990).

171. Article 8(1) provides: "Everyone has the right to respect for his private and family life, his home and his correspondence." [European] Convention for the Protection of Human Rights and Fundamental Freedoms, *opened for signature* Nov. 4, 1950, art. 8(1), Europ. T.S. No. 5, 213 U.N.T.S. 221, 230 (entered into force Sept. 3, 1953) [hereinafter European Convention]. Article 8(2) further states:

> There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

172. Article 8(1) provides: "Everyone has the right to the protection of personal data concerning him or her." Charter of Fundamental Rights of the European Union art. 8, ¶ 1, 2000 O.J. (C 364) 1, 10. Although the Charter is not legally binding upon the Member States, it has occasionally influenced decisions of the European Court of Justice. *See NBSP Report*, *supra* note 53, at 36.

173. Article 10 provides: "Everyone has the right to respect for private life in relation to information about his or her health." Convention for the Protection of Human Rights and Dignity of the Human Being with Regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine art. 10, Apr. 4, 1997, E.T.S. No. 164, *available at* http://conventions.coe.int/Treaty/EN/Treaties/html/164.htm. Article 23 states: "The Parties shall provide appropriate judicial protection to prevent or to put a stop to an unlawful infringement of the rights and principles set forth in this Convention at short notice." *Id*. art. 23.

174. Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data art. 7, Jan. 28, 1981, E.T.S. No. 108, *available at* http://conventions.coe.int/Treaty/EN/Treaties/Html/108.htm ("Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised

B. Collection of Biometric Information

1. United States: Fingerprinting and the Fourth Amendment

The privacy interests of refugees and asylum seekers in the United States find protection under the Fourth and Fourteenth Amendments to the United States Constitution.[176] The Fourth Amendment protects "[t]he right of people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures."[177] Its "overriding function . . . is to protect personal privacy and dignity against unwarranted intrusion by the State."[178] The Fourth Amendment is violated when the government conducts an unreasonable search. Since government action is present in requiring the collection of biometric information from refugees, even if those who collect it are private actors,[179] the first important issue is whether fingerprinting constitutes a search under the Fourth Amendment.

A search occurs under the Fourth Amendment when "an expectation of privacy that society is prepared to consider reasonable is infringed."[180] In assessing the reasonableness of an individual's privacy interests, courts may consider: the location of the individual

---

destruction or accidental loss as well as against unauthorised access, alteration or dissemination.").

175. *See* EU Privacy Directive *supra* note 160; Council and Parliament Directive 2002/58/EC, Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, 2002 O.J. (L 201) 37 (also referred to as the e-Privacy Directive).

176. "The fourteenth amendment to the constitution is not confined to the protection of citizens. . . . [Its] provisions are universal in their application, to all persons within the territorial jurisdiction, without regard to any differences of race, of color, or of nationality; and the equal protection of the laws is a pledge of the protection of equal laws." Yick Wo v. Hopkins, 118 U.S. 356, 369 (1886).

177. U.S. Const. amend. IV.

178. Schmerber v. California, 384 U.S. 757, 767 (1966).

179. *See* Greg Star, *Airport Security Technology: Is the Use of Biometric Identification Technology Valid Under the Fourth Amendment?*, 20 Temp. Envtl. L. & Tech. J. 251, 257 (2002) (collection of biometric information by airline employees constitutes government action and thus implicates the Fourth Amendment, if the collection is a search).

180. Maryland v. Macon, 472 U.S. 463, 469 (1985) (quoting United States v. Jacobsen*,* 466 U.S. 109, 113 (1984)) (internal quotation marks omitted) (finding respondent lacked reasonable expectation of privacy in areas of a store open to the public).

asserting the privacy interest,[181] the legal relationship between the individual and the state,[182] the extent to which the search threatens the individual's safety or health,[183] and the nature and extent of the intrusion upon the individual's "dignitary interests in personal privacy and bodily integrity."[184] If an individual is found to have a reasonable privacy interest, that interest must be balanced against the legitimate interests of the government in effectuating the search.[185]

Although the Supreme Court has suggested that the collection of biometrics, specifically fingerprinting, does not constitute a search under the Fourth Amendment, the matter is not entirely clear. In *Davis v. Mississippi*, the Supreme Court found "no merit in the suggestion . . . that fingerprint evidence, because of its trustworthiness, is not subject to the proscriptions of the Fourth and Fourteenth Amendments."[186] However, the court proceeded to distinguish fingerprinting from recognized searches in that fingerprinting (1) "involves none of the probing into an individual's private life and thoughts that marks an interrogation or search," (2) cannot be repeatedly collected "to harass any individual, since the police need only one set of each person's prints," and (3) "is an inherently more reliable and effective crime-solving tool than eyewitness identifications or confessions and is not subject to such abuses as the improper line-up and the 'third degree.'" [187] The

181. *See* Vernonia School Dist. 47J v. Acton, 515 U.S. 646, 654 (1995) ("What expectations [of privacy] are legitimate varies, of course, with context, . . . depending, for example, upon whether the individual asserting the privacy interest is at home, at work, in a car, or in a public park.").

182. *See, e.g.*, *id.* (quoting Griffin v. Wisconsin, 483 U.S. 868, 873, 875 (1987)) ("[A]lthough a 'probationer's home, like anyone else's, is protected by the Fourth Amendmen[t],' the supervisory relationship between probationer and State justifies 'a degree of impingement upon [a probationer's] privacy that would not be constitutional if applied to the public at large.'").

183. Winston v. Lee, 470 U.S. 753, 753–54 (1985) (holding "the extent to which . . . [a] procedure may threaten the individual's safety or health" is a factor for determining the reasonableness of the search).

184. *Id.* at 754.

185. *Vernonia*, 515 U.S. at 652–53 (citing Skinner v. Ry. Labor Execs.' Ass'n, 489 U.S. 602, 619 (1989)); *see also* Terry v. Ohio, 392 U.S. 1, 20–21 (1968) (holding that the test for reasonableness of a search involves balancing the governmental interest in the search against the interests of the individual against invasion).

186. Davis v. Mississippi, 394 U.S. 721, 723–24 (1969) (holding that fingerprints obtained during an illegal detention should have been excluded).

187. *Id.* at 727.

Supreme Court later held that the Fourth Amendment does not extend protection to "[w]hat a person knowingly exposes to the public,"[188] and has characterized fingerprints as such.[189]

Given this constitutional background, the fingerprinting of refugees and asylum seekers appears unlikely to be considered a search under the Fourth Amendment. The use of fingerprinting has "long been recognized as a scientific and accurate means of identification."[190] Fingerprinting is pervasive and is required by numerous state and federal laws in a number of non-criminal contexts, including, for example, federal securities law[191] and for employment in bartending,[192] day care,[193] and real estate sales.[194] Noting the widespread use of fingerprints, the district court in *Thom* remarked, "to suggest that a stigma attaches when it is so used is to fly in the face of reality."[195] As to its perceived affect upon the individual, the same court stated that the "actual inconvenience is minor; the claimed indignity, nonexistent; detention, there is none; nor unlawful search; nor unlawful seizure."[196] A minority of courts have reached the opposite conclusion, however, holding that

188. Katz v. United States, 389 U.S. 347, 351 (1967).

189. Cupp v. Murphy, 412 U.S. 291, 295 (1973) (distinguishing fingerprinting, as a search of publicly-exposed physical characteristics, from a search of fingernails).

190. Thom v. N.Y. Stock Exchange, 306 F. Supp. 1002, 1006 (S.D.N.Y. 1969) (upholding statute requiring all employees of firms of national securities exchanges registered with the Securities and Exchange Commission to submit to fingerprinting).

191. 15 U.S.C. § 78q(f)(2) (2006) ("Every member of a national securities exchange, broker, dealer, registered transfer agent, and registered clearing agency, shall require that each of its partners, directors, officers, and employees be fingerprinted and shall submit such fingerprints, or cause the same to be submitted, to the Attorney General of the United States for identification and appropriate processing.").

192. *See* Iacobucci v. City of Newport, 785 F.2d 1354 (6th Cir. 1986) (holding that city ordinance requiring employees at places where liquor is served to be fingerprinted by the police was not unconstitutional), *rev'd on other grounds*, 479 U.S. 92 (1986).

193. Cal. Health & Safety Code § 1596.871(a), (b)(1)(A)–(D), (c)(1) (2006). Certain exemptions exist. *Id*.

194. *See* Hamilton v. N.J. Real Estate Comm'n, 284 A.2d 564 (N.J. Super. Ct. App. Div. 1971) (holding that regulation by the Real Estate Commission requiring the fingerprinting of current and prospective salespersons, brokers, and broker-salespersons is not unconstitutional).

195. *Thom*, 306 F. Supp. at 1009.

196. *Id.*

fingerprinting constitutes a search within the meaning of the Fourth Amendment.[197]

However, developments in the science of biometrics may give the Supreme Court reason to reconsider its increasingly dated jurisprudence on biometrics and the Fourth Amendment. Several scientific studies suggest that fingerprints and other biometrics may incidentally reveal medical information about an individual.[198] For example, certain chromosomal disorders, such as Down syndrome, Turner syndrome, and Klinefelter syndrome, are "known to be associated with characteristic dermatoglyphic abnormalities."[199] Certain fingerprint patterns also implicate some non-chromosomal disorders, including chronic intestinal pseudo-obstruction, leukemia, breast cancer, and Rubella syndrome.[200] The Supreme Court in *Skinner v. Ry. Labor Executives' Ass'n* recognized that the collection and testing of urine and blood "can reveal a host of private medical facts about an [individual]"[201] and thereby "intrudes upon expectations of privacy that society has long recognized as reasonable . . . [and] must be deemed searches under the Fourth Amendment."[202] It may then be argued that the collection of biometrics should also be considered a search because fingerprints may also contain such private medical facts.[203]

If fingerprinting is deemed a search under the Fourth Amendment, will it be considered reasonable? The Fourth Amendment prohibits searches that are unreasonable.[204] Despite the government's considerable interest in promoting public safety and

197. *See* Hooker v. State, 92-KA-00242-SCT, 716 So. 2d 1104, 1112 (Miss. 1998) (interpreting Davis v. Mississippi, 394 U.S. 721 (1969), as holding that fingerprinting is a search under the Fourth Amendment); *see also* Paulson v. Florida, 360 F. Supp. 156, 161 (S.D. Fla. 1973) (emphasizing that fingerprinting itself "constitutes a seizure of evidence fully subject to the constraints of the fourth amendment").

198. *See* John D. Woodward, Jr., *Biometrics: Identifying Law & Policy Concerns*, *in* Biometrics: Personal Identification in Networked Society 385, 393 (Anil Jain & Ruud Bolle eds., 1998).

199. *Id.*

200. *See id*. *See also* Johns Hopkins Physicians Update, *Gastroenterology: Fingerprinting GI Disease* 5 (Apr. 1996) (explaining the discovery of a relationship between an uncommon fingerprint pattern, known as a digital arch, and a medical disorder called CIP which affects 50,000 people nationwide).

201. Skinner v. Ry. Labor Executives' Ass'n, 489 U.S. 602, 617 (1989).

202. *Id.*

203. *See* Star, *supra* note 179, at 257–61.

204. U.S. Const. amend. IV.

national security,[205] searches conducted without a warrant based upon probable cause are "*per se* unreasonable . . . subject only to a few specifically established and well-delineated exceptions."[206] In other words, only the application of an exception makes a search reasonable in the absence of a warrant based upon probable cause. Assuming that fingerprinting constitutes a search under the Fourth Amendment, two exceptions would be of particular relevance: consent and the border search exception. Each will be discussed in greater detail.

It may be argued that refugees and asylum seekers consent to fingerprinting requirements for visa applications, public assistance, or asylum. However, consent must be given voluntarily to be counted as reasonable.[207] Whether consent to a search is voluntary depends on a consideration of the totality of the circumstances, including "the possibly vulnerable subjective state of the person who consents."[208] Those fleeing from a well-founded fear of persecution are undoubtedly in a vulnerable subjective state. Moreover, the Fourth and Fourteenth Amendments have been interpreted to mandate that consent "not be coerced, by explicit or implicit means, by implied threat or covert force."[209] Since obtaining consent from refugees and asylum seekers who believe they will be removed if they do not consent may be inherently threatening, the consent exception should almost never apply. Consequently, the fingerprinting of asylum seekers as a condition of their obtaining asylum may be unreasonable, assuming, of course, that fingerprinting constitutes a search under the Fourth Amendment.

When refugees' and asylum seekers' fingerprints are enrolled through the US-VISIT system, the border search exception likely applies. The Supreme Court stated "[t]ime and again . . . that 'searches made at the border, pursuant to the longstanding right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border.'"[210] Congress has thereby "granted the Executive plenary authority to conduct routine searches

205. *See supra* note 20 and accompanying text.

206. Katz v. United States, 389 U.S. 347, 357 (1967).

207. Schneckloth v. Bustamonte, 412 U.S. 218, 223 (1973) (presenting the question of how the prosecution must show consent was voluntary).

208. *Id.* at 226, 229.

209. *Id.* at 228.

210. United States v. Flores-Montano, 541 U.S. 149, 152–53 (2004) (quoting United States v. Ramsey, 431 U.S. 606, 616 (1977)).

and seizures at the border, without probable cause or a warrant."[211] The exception applies either at the border itself or at its "functional equivalent," which includes international airports.[212] The Fourth Amendment therefore authorizes "routine searches and seizures" at the border or its "functional equivalent."

The issue then becomes whether fingerprinting, assuming it constitutes a search under the Fourth Amendment, qualifies as a *routine search*. Discussing the propriety of searching vehicles at the border, the Supreme Court disavowed "[c]omplex balancing tests to determine what is a 'routine' vehicle search."[213] The court has recognized that more intrusive searches, such as those involving incursions into an individual's alimentary canal, require reasonable suspicion to pass Fourth Amendment muster.[214] However, it has declined to decide "what level of suspicion, if any, is required for non-routine border searches such as strip, body-cavity, or involuntary x-ray searches."[215]

Against this background, a court would be hard-pressed to hold fingerprinting to be anything other than routine. Fingerprinting has been widely used in the United States since 1902,[216] and it is widely used today with millions of individuals fingerprinted at the U.S. border and ports of entry each year.[217] A court following the Supreme Court's reasoning in *Davis v. Mississippi* would likely deem the collection of fingerprints relatively unobtrusive.[218] Therefore, even assuming that fingerprinting constitutes a search, fingerprinting refugees and asylum seekers at the border would likely comport with the requirements of the Constitution.

---

211. United States v. Montoya de Hernandez, 473 U.S. 531, 537 (1985) (citing *Ramsey*, 431 U.S. at 616–17 (citing Act of July 31, 1789, ch. 5, 1 Stat. 29)).

212. Almeida-Sanchez v. United States, 413 U.S. 266, 273 (1973) ("[A] search of the passengers and cargo of an airplane arriving at a St. Louis airport after a nonstop flight from Mexico City would clearly be the functional equivalent of a border search.").

213. *Flores-Montano*, 541 U.S. at 152 (citation omitted) (discussing the inspection of a vehicle's gas tank followed by removal).

214. *Montoya de Hernandez*, 473 U.S. at 541 (finding that an alimentary canal search at an international border can be justified by "reasonable suspicion").

215. *Id.* at 546 n.4.

216. *See supra* note 132 and accompanying text.

217. *See supra* note 17 and accompanying text.

218. *See supra* note 186 and accompanying text.

2. European Union

The Member States of the European Union "have moved aggressively to regulate the use of personal data."[219] Their efforts are embodied in the European Parliament and Council Directive 95/46/EC (the EU Privacy Directive),[220] which recognizes the "right to privacy with respect to the processing of personal data" as one of the "fundamental rights and freedoms of natural persons."[221] The Privacy Directive offers "high levels of protection,"[222] generally prohibiting the "processing of personal data," which almost certainly includes the collection of biometric information,[223] where the person from whom the data is to be collected has not "unambiguously given his consent."[224] However, in certain specified situations, such as when "processing is necessary for the performance of a task carried out in the public interest," the processing of personal data can occur without obtaining consent.[225] Thus, the Privacy Directive provides

219. Julia M. Fromholz, *The European Union Data Privacy Directive*, 15 Berkeley Tech. L.J. 461, 461 (2000).

220. *See* EU Privacy Directive, *supra* note 160. Each member state must pass its own implementing legislation to effect the protections of the Privacy Directive. *See* Borchardt, Community Law, *supra* note 47, at 65 ("A directive is binding on the Member States as regards the objective to be achieved but leaves it to the national authorities to decide on how the agreed Community objective is to be incorporated into their domestic legal systems."); *see also* Fromholz, *supra* note 219, at 468 (explaining that harmonization of data privacy laws in the EU is linked to protection of fundamental human rights, including the right to privacy).

221. *See* EU Privacy Directive, *supra* note 160, art. 1(1). Privacy interests also find protection in the European Convention, *see supra* note 171, and the Charter of Fundamental Rights of the European Union. *See supra* note 172.

222. Fromholz, *supra* note 219, at 468.

223. The EU Privacy Directive defines "processing of personal data" to include "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction." EU Privacy Directive, *supra* note 160, art. 2(b). The Directive's preamble states that "the principles of protection must apply to any information concerning an identified or identifiable person" and "to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person." *Id.* pmbl. ¶ 26. Refugees' and asylum seekers' biometric information will "most certainly" be considered "personal data" meriting protection under the Directive because such information concerns an identified or identifiable person. *See NBSP Report*, *supra* note 53, at 26.

224. EU Privacy Directive, *supra* note 175, art. 7(a).

225. *Id.* art. 7(e).

Member States ample authority to collect refugees' and asylum seekers' biometric information, either at national borders or otherwise.

C. Retention of Biometric Information

The storage of biometric records raises obvious privacy concerns, but it also raises concerns particular to refugees and asylum seekers. This section discusses these concerns, comparing United States and European Union practices where relevant. This section argues in favor of implementing measures to restrict the transfer of biometric information stored in databases maintained by DHS and other agencies. It further argues that the retention period for refugees' and asylum seekers' biometric information is unnecessarily long, threatens refugees' and asylum seekers' privacy and security, and consequently should be shortened.

1. Need for Security and Confidentiality

According to UNHCR, "[c]onfidentiality of data is particularly important for refugees and other people in need of international protection, as there is a danger that agents of persecution or rights violations may ultimately gain access to such information, potentially exposing a refugee to danger even in his/her asylum country."[226] The

226. *UNHCR Comments*, *supra* note 58, at 19. Forcibly returned refugees and failed asylum seekers sometimes face persecution from their state of origin. For example, Amnesty International has received reports that North Koreans forcibly returned from China "face long interrogation sessions and torture," and some are sent to prison or labor camps, "receiving meagre food rations, contracting illnesses and being denied access to medical care." Amnesty Int'l, *Democratic People's Republic of Korea, Persecuting the Starving: The Plight of North Koreans Fleeing to China*, 9–10, AI Index ASA 24/003/2000 (Dec. 15, 2000), *available at* http://www.unhcr.org/refworld/docid/3b83b6fb0.html. The families of forcibly returned refugees are also reported to face punishment at the hands of the North Korean authorities. *Id.* at 10. Thus, even if a North Korean refugee is not forcibly returned to North Korea, the release of information tending to show that the individual crossed a national border or applied for asylum threatens the safety of his or her family. Human rights organizations have reported the persecution of the families of refugees in other contexts. *See, e.g.*, Human Rights Watch, Uzbekistan: Stop Persecuting Andijan Refugees' Families (May 4, 2010), http://www.unhcr.org/refworld/docid/4be90b77c.html (calling on Uzbekistan to stop harassing the families of Andijan refugees, including subjecting them to constant surveillance, regular police interrogations, arbitrary arrests, and ill-treatment while in custody); Human Rights Watch, *Service for Life: State Repression and Indefinite Conscription in Eritrea* 75 (Apr. 2009),

implementation of an adequate data protection system and the assurance that biometric information will not be transferred to third countries would address these concerns. However, such assurances are lacking. DHS reports that "IDENT shares data with . . . foreign or international government agencies charged with . . . law enforcement, immigration, intelligence, or other DHS mission-related functions."[227] Sharing is to take place "after DHS determines that the receiving agency has a need to know the information" and then "only to the extent permissible by law."[228] Nevertheless, this willingness to share refugees' and asylum seekers' immutable biometric data increases the likelihood that such data will fall into the wrong hands.

In this respect, the European Union's Eurodac affords a higher degree of data protection than its American analogues. A person from whom biometric data is taken has a right to be informed of the recipients of her data.[229] The central unit of Eurodac cannot transfer biometric data to third countries, "unless it is specifically authorized to do so in the framework of a Community agreement."[230] The Privacy Directive provides that transfer of personal data to a third country "may take place only if . . . the third country in question ensures an *adequate* level of protection."[231] The adequacy of a third country's protections are to "be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations," including "the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law . . . in force in the third country in question and the [third country's] professional rules and security measures."[232] Where a third

---

available at http://www.hrw.org/en/node/82280/section/1 ("If refugees or other Eritrean expatriates do not pay the two percent tax [imposed on the diaspora] then the government typically punishes family members in Eritrea by arbitrarily detaining them, extorting fines, and denying them the right to do business by revoking licenses or confiscating land.").

227. IDENT PIA, *supra* note 18, at 8.

228. BSS PIA, *supra* note 22, at 11. DHS also reported that a memorandum of understanding was being drafted to "address specific confidentiality protections provided to certain classes of applicants for example, asylum seekers," but the author has not been able to locate the MOU. *Id.* at 12.

229. Eurodac Regulation, art. 18(1)(c), *supra* note 35, at 8. A proposal to amend Eurodac would further increase its transparency by requiring lists of the authorities with access to Eurodac to be published in the European Union's Official Journal. *See UNHCR Comments*, *supra* note 58, at 23.

230. Eurodac Regulation, *supra* note 35, art. 15(5).

231. EU Privacy Directive, *supra* note 160, art. 25(1) (emphasis added).

232. *Id.* art. 25(2).

country is determined to lack adequate protections, the Directive requires Member States to "inform each other" of their determination and "take the measures necessary to prevent any transfer of data of the same type to the third country in question."[233] Although the Directive contains a number of narrow exceptions that enable Member States to transfer personal data notwithstanding a third country's lack of adequate safeguards,[234] it also establishes a framework for reporting and challenging certain potentially problematic derogations.[235] A reevaluation of the DHS practice of sharing biometric information with foreign governments and international agencies, perhaps bringing them in line with those of Eurodac, would do much to protect the largely immutable biometric identity of refugees and asylum seekers in the United States.

With respect to the implementation of an adequate protection system, DHS maintains that IDENT is protected by a "rigorous security program employing physical, technical, and administrative controls,"[236] and that data shared with external organizations "must be kept secure, accurate, and appropriately controlled" through a variety of means.[237] Such efforts are likely necessary under the Privacy Act of 1974,[238] which requires that federal agencies "establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained."[239]

233. *Id.* art. 25(3)–(4).

234. *See id.* art. 26(1)–(2).

235. *See id*. art. 26(3)–(4).

236. IDENT PIA, *supra* note 18, at 16.

237. *Id.* at 9 ("[P]rivacy risks are mitigated through data sharing agreements that require such things as auditing, access controls, re-sharing limits, and other physical, technical, and administrative controls.").

238. Privacy Act of 1974, Pub. L. No. 93-578 (codified as amended at 5 U.S.C. § 552a (2006)).

239. *Id.* § 552a(e)(10). "Record" is defined broadly to include any "other identifying particular assigned to the individual, such as a finger or voice print or a photograph." *Id.* § 552a(a)(4). The Act also establishes rules of conduct governing those who develop or maintain a system of records. *Id.* § 554a(e)(9).

2. Duration of Storage

Refugees' and asylum seekers' biometric information should be retained no longer than necessary. An excessively long period of retention is undesirable because it increases the possibility that data may be shared and ultimately misused.[240] Biometric records stored in IDENT are retained for seventy-five years or until the statute of limitations for all criminal violations has expired.[241] As discussed above, records stored in IDENT include information collected by US-VISIT and numerous programs both internal and external to DHS,[242] and biometric information collected from asylum seekers at Application Support Centers are compared against IDENT.[243] In contrast, biometric records contained in the European Union's Eurodac and the United Kingdom's IAFIS are stored for no longer than ten years from the date on which the fingerprints were taken.[244] DHS has acknowledged the possibility that biometric data transferred to other agencies may be used for the purpose of data-mining, whereby the aggregation of data can "result in information that exceeds the specific purposes the separate data elements were collected for in the first place."[245] DHS has further acknowledged that an aggregate collection of data "may be a more valuable and attractive target."[246] As a result, DHS has stated that it is "currently undertaking a reevaluation of the retention policy . . . and may determine a new retention period or combination of retention periods dependent upon the data collected."[247]

3. Potential to Block Meritorious Applications

Human rights groups have criticized the collection and storage of refugees' and asylum seekers' biometric data, arguing that the existence of biometric identifiers automatically linking applicants to past asylum applications should not preclude their new

240. For examples of how sharing biometric information may threaten the safety of refugees, asylum seekers, and their families, see *supra* note 226.

241. IDENT PIA, *supra* note 18, at 6.

242. *See supra* note 30 and accompanying text.

243. *See supra* note 23 and accompanying text.

244. *See supra* notes 39 & 93 and accompanying text.

245. IDENT PIA, *supra* note 18, at 4.

246. *Id.*

247. *Id.* at 7.

applications.[248] After all, unsuccessful asylum seekers' circumstances can change and give rise to legitimate claims of asylum. Unless safeguards are put into place, it is feared that "the impact of biometrics will be to push more refugees . . . into resorting to irregular forms of migration"[249] or self-mutilation.[250] A recent proposal to amend the Dublin II Regulation to require that Member States grant asylum seekers personal interviews would help mitigate this risk.[251] The need for such protective measures is especially great in the United States due to its much longer retention period, throughout which unsuccessful asylum applicants' circumstances can change tremendously.

4. *S. and Marper v. United Kingdom*: A Recent Challenge to the Retention of Biometric Information

Few cases squarely address the privacy interests implicated by the retention of biometric information, but in *S. and Marper v. United Kingdom*, the European Court of Human Rights held that the indefinite retention of cellular samples and DNA and fingerprint profiles of persons acquitted or persons having their prosecution discontinued violated Article 8 of the European Convention on Human Rights (European Convention).[252] Although the dispute arose in the criminal context, it nonetheless contains important clues as to how the court would rule on the legality of retaining the fingerprints and DNA samples of refugees and asylum seekers. The court stated that the retention of cellular samples "*per se* must be regarded as

248. *See* ECRE, Defending Refugees' Access, *supra* note 162, at 33 (explaining how biometrics could pose an additional hurdle to asylum in the EU).

249. *Id.*

250. *Sweden Refugees Mutilate Fingers*, BBC News (Apr. 2, 2004), http://news.bbc.co.uk/2/hi/europe/3593895.stm (reporting how asylum seekers avoided biometric identification based on previous asylum requests through mutilation, and quoting one identity expert of the Swedish Migration Board who stated, "[w]e see everything scars [sic] from knives and razors, or entire [fingerprint] patterns that are entirely destroyed because they've used acid or some other kind of product to destroy their hands").

251. *UNHCR Comments*, *supra* note 58, at 15.

252. S. v. United Kingdom, App. Nos. 30562/04 and 30566/04, 48 Eur. H.R. Rep. 50, ¶¶ 77, 86 (2009). Although at least twenty Member States practiced collecting and retaining criminal suspects' DNA information, no state besides the United Kingdom allowed for indefinite retention of samples upon acquittal or the discontinuance of criminal proceedings, but some states would allow as much only in certain narrow circumstances, such as when there is a risk that the suspect will commit a serious crime. *Id.* ¶¶ 45–47.

interfering with the right to respect for the private lives of the individuals concerned."[253] It also found that the retention of fingerprints under such circumstances "constitute[d] an interference with the right to respect for private life."[254]

The Court then considered whether the United Kingdom's interference with the petitioners' right to private life was authorized under Article 8(2) of the European Convention. It focused upon whether the interference was "in accordance with the law," for a "legitimate purpose," and "necessary in a democratic society."[255] In evaluating whether the interference was necessary in a democratic society, the Court considered whether it "answer[ed] a pressing social need," which was "proportionate to the legitimate aim pursued" and supported by reasons "relevant and sufficient."[256] Recognizing that these issues ought to ordinarily be decided by national authorities, the Court afforded the respondent a "margin of appreciation," but it limited the breadth of this margin after noting the "fundamental importance" of the rights at stake.[257]

In finding that the United Kingdom overstepped its margin of appreciation, the court accepted the usefulness of biometrics in combating crime as "beyond dispute" and thereby addressed a legitimate public need.[258] However, it nonetheless found that this particular application of biometrics on acquitted persons was disproportionate to the legitimate aim of combating crime.[259] Although the Court has not addressed the legality of Eurodac, it would likely hold the limited duration of retention, coupled with the legitimate concerns of the Member States in preventing fraud, to be proportionate, "necessary in a democratic society," and therefore authorized under Article 8(2) of the European Convention. Still, the privacy concerns addressed by the Court, and their explicit association with the protection and storage of biometric information, are relevant for all countries that collect biometric data on refugees and asylum seekers.

---

253. *Id.* ¶ 73 (emphasis added).
254. *Id.* ¶ 86.
255. *Id.* ¶¶ 95–126.
256. *Id.* ¶ 101.
257. "The margin will tend to be narrower where the right at stake is crucial to the individual's effective enjoyment of intimate or key rights." *Id*. ¶ 102.
258. *Id.* ¶ 105.
259. *Id.* ¶¶ 125–26.

D. Misidentification

As with other human endeavors, the identification of individuals by their fingerprints is not problem-free. This section does not challenge the technical and scientific bases underlying fingerprint identification, nor does it dispute the proposition that fingerprint identification is generally accurate where administered properly. However, it is appropriate to note that misidentification threatens serious harm, not only to refugees and asylum seekers, who might be turned away at ports of entry, denied asylum, or deprived of other life-saving aid, but also to persons facing criminal conviction on the basis of fingerprint evidence. However, it should be stated from the outset that one of the most controversial aspects of fingerprint evidence in criminal proceedings, the use of latent prints,[260] is not present here because refugees and asylum seekers have their prints directly taken by the authorities.[261] The threat of misidentification instead stems from the combination of technical and human error.

Although there is scientific and empirical support for the proposition that fingerprints are unique to the individual,[262] it does not follow that print-matching software, or its human operators, is capable of comparing and matching the prints of millions of individuals with complete accuracy.[263] Indeed, some commentators

260. Latent prints are prints "left by substances such as sweat, oil, or blood on the friction ridges and deposited on a surface, such as glass, paper, or the metal surface of a gun." Lisa J. Steele, *The Defense Challenge to Fingerprints*, 40 Crim. Law Bulletin 213, 219 (2004). A technician must use "a variety of powders and materials" to make the print visible and to record it. *Id.* The use of latent prints may lead to misidentification because latent prints "may exhibit only a small portion of the surface of the finger and may be smudged, distorted, or both, depending on how they were deposited." Sandy L. Zabell, *Fingerprint Evidence*, 13 J.L. & Pol'y 143, 144 (2005).

261. *See supra* notes 15, 21 and accompanying text.

262. A study by Stephen Meagher of the FBI's Latent Fingerprint Section compared 50,000 digitally stored fingerprints to one another and concluded that the chances of misidentification were extremely small, at 1 in 10^{97}. The study was subsequently criticized for failing to reflect real-world conditions. *See* Andy Coghlan & James Randerson, *How Far Should Fingerprints be Trusted?*, New Scientist, Sept. 19, 2005, at 3.

263. *See, e.g.*, *Strengthening Forensic Science in the United States: Hearing Before the S. Comm. on the Judiciary*, 111th Cong. 3 (2009) (statement of the Honorable Harry T. Edwards, Senior Circuit Judge and Chief Judge Emeritus, United States Court of Appeals for the D.C. Circuit and Visiting Professor of Law, New York University School of Law and Co-Chair, Committee on Identifying the Needs of the Forensic Science Community The Research Council

and practitioners have complained of "the dearth of solid research to establish the limits and measures of performance and to address the impact of the sources of variability and potential bias in most disciplines."[264] Nevertheless, "courts have been led to believe that disciplines such as fingerprinting stand on par with DNA analysis."[265] The Seventh Circuit favorably referenced the testimony of an FBI fingerprint expert, stating "that the error rate for fingerprint comparison is essentially zero."[266] That decision was cited approvingly by the Fourth Circuit.[267]

A challenge to the admissibility of fingerprints collected from asylum applicants through Eurodac was recently considered in the United Kingdom. In *RZ v. Secretary of State for the Home Department*, the UK Asylum and Immigration Tribunal upheld the Secretary's introduction of Eurodac fingerprints to undermine the applicant's contention that he had not left Eritrea prior to his arrival in the U.K.[268] Matching fingerprints had previously been taken in Italy and tended to show that the applicant had illegally crossed the Italian border.[269] The tribunal concluded that, in light of the safeguards within the Eurodac system, fingerprints stored within Eurodac "should be accepted as accurate and reliable," unless there appears "cogent evidence" to the contrary.[270] Although the tribunal

---

of the National Academies), http://judiciary.senate.gov/pdf/09-03-18EdwardsTestimony.pdf [hereinafter Strengthening Forensic Science] ("A 'zero error rate' is a myth in fingerprint analyses and in all other forensic disciplines."); European Commission Directorate-General Joint Research Centre, *Biometrics at the Frontiers: Assessing the Impact on Society*, at 10 (Feb. 2005), ftp://ftp.jrc.es/pub/EURdoc/eur21585en.pdf ("[B]iometric identification is not perfect—it is never 100% certain, it is vulnerable to errors and it can be 'spoofed.'").

264. Strengthening Forensic Science, *supra* note 263, at 3.

265. *Id.*

266. United States v. Havvard, 260 F.3d 597, 599 (7th Cir. 2001). *But see* David Stout, *Report Faults F.B.I.'s Fingerprint Scrutiny in Arrest of Lawyer*, N.Y. Times, Nov. 17, 2004, at A18 (describing a report by the Office of the Inspector General in connection with the misidentification of immigration lawyer Brandon Mayfield and the subsequent implication of his involvement in the Madrid bombings of 2004). "The error was a human error and not a methodology or technology failure. . . . Once the mind-set occurred with the initial examiner, the subsequent examinations were tainted." *Id.*

267. United States v. Crisp, 324 F.3d 261, 269 (4th Cir. 2003).

268. RZ v. Secretary of State for the Home Department [2008] UKAIT 00007, *available at* http://www.ait.gov.uk/Public/Upload/j2093/00007_ukait_2008_rz_eritrea.doc.

269. *Id.* ¶ 4.

270. *Id.* ¶ 2.

placed the burden of proving fingerprint matches on the government, it held the government need not provide corroboration, establish the continuity of the evidence, or provide the court with the credentials of the technician who recorded the biometric.[271]

There are, however, several potential sources of inaccuracy in fingerprint identification. First, the "accuracy, completeness, and quality [of fingerprints stored in IDENT] may vary considerably" because of the "diverse environments" in which fingerprints are collected.[272] The same is true about the fingerprints stored in Eurodac.[273] Second, in some cases, "[a]n individual's age and occupation may cause some sensors difficultly in capturing a complete and accurate fingerprint image."[274] Third, automated fingerprint identification systems do not function without the assistance and input of human technicians, and while they "are very good at winnowing an enormous database into a small group of candidate matches . . . they are relatively poor at picking which, if any, of this small group is the actual match."[275] Such systems compare visual images by executing a number of rules and leave it to human examiners to select "the true matching print" from a list of computer generated candidate matches.[276]

Fourth, the involvement of human operators necessarily increases the possibility of error, particularly where the operators lack training.[277] According to one commentator, the switch from storing fingerprints on a card to digital storage has made it unclear how "novice fingerprint examiners [will] acquire the visual skills" of their predecessors, since the retrieval of fingerprint cards was a

271. *Id.* ¶ 50.

272. IDENT PIA, *supra* note 18, at 5. While promulgating minimum data quality standards and conducting quality checks can alleviate the problem, "it is ultimately the responsibility of the data owner . . . to ensure the accuracy, completeness, and quality of the data." *Id.*

273. *See* Eurodac Regulation, *supra* note 35, at 4 ("The procedure for taking fingerprints shall be determined in accordance with the national practice of the Member State concerned and in accordance with the safeguards laid down in the European Convention on Human Rights and in the United Nations Convention on the Rights of the Child.").

274. National Science & Technology Council, Subcommittee on Biometrics, Biometrics Frequently Asked Questions 4 (2006), *available at* www.biometrics.gov/Documents/FAQ.pdf [hereinafter Biometrics FAQ].

275. Cole, Suspect Identities, *supra* note 132, at 255.

276. *Id.* at 256.

277. *See* Biometrics FAQ, *supra* note 274, at 15 (stating that the accuracy of some biometrics is "to some degree" dependent on the human operator).

"training ground for examiners."[278] Finally, human operators are subject to contextual biases. One study presented fingerprint examiners with prints that had been accurately identified in the past, and then subjected the examiners to context bias by telling them, for example, that the suspect from whom the fingerprints had been taken had confessed.[279] The study revealed that one-third of such examiners rendered a false positive.[280] A list of potential matches generated by an automated fingerprint identification system may create such bias, suggesting that its operator should choose among the prints provided rather than none at all. Given the magnitude of the interests of refugees and asylum seekers, this Note urges caution in the operation of automated fingerprint identification systems and the subsequent review of matches by courts and other decisionmakers.[281]

E. Reluctance to Undergo Fingerprinting

Greater effort should be made to inform refugees and asylum seekers of the purpose behind collecting their biometric information and to assure them that their information will not be misused. For refugees and asylum seekers, the collection of biometric information may be an uncomfortable or alarming experience. Such apprehension stems primarily from the stigma of criminality and perceived punitive intent,[282] which are compounded by reports of widespread hostility towards refugees and asylum seekers.[283] Although reluctance to undergo fingerprinting tends to receive little sympathy in the United States,[284] opposition to fingerprinting is well-

278. Cole, Suspect Identities, *supra* note 132, at 256–57. A proficiency test administered by the International Association for Identification (IAI) and the Collaborative Testing Service (CTS) revealed that of 156 examiners employed in American police crime labs, only 44% scored perfectly and 22% reported false positives. *Id.* at 281.

279. *See* Strengthening Forensic Science, *supra* note 263, at 3–4.

280. *See id.*

281. A degree of judicial skepticism of seemingly neutral, scientific evidence might also be warranted. *See* Melendez-Diaz v. Massachusetts, 129 S. Ct. 2527, 2536 (2009) ("Nor is it evident that what respondent calls 'neutral scientific testing' is as neutral or as reliable as respondent suggests.").

282. UNHCR Handbook for Registration, *supra* note 147, at 86.

283. *See supra* notes 163–164 and accompanying text.

284. *See, e.g.*, Thom v. New York Stock Exchange, 306 F. Supp. 1002, 1007 (S.D.N.Y. 1969) ("The day is long past when fingerprinting carried with it a stigma or any implication of criminality."); U.S. v. Kincade, 379 F.3d 813, 874 (9th Cir. 2004) (Kozinski, J., dissenting) ("[W]e have come to accept that

documented in some societies. For example, fingerprinting carries a considerable stigma in Japan,[285] leading human rights groups to protest the promulgation of the Law for Partial Amendment of the Immigration Control and Refugee Recognition Act, which mandates fingerprinting of most foreign visitors and residents.[286]

UNHCR has recognized the necessity of overcoming cultural sensitivities to fingerprinting, and its *Handbook for Registration* instructs UNHCR Protection Officers to "[o]rganize meetings with both women and men of the refugee community to discuss issues related to registration and documentation"[287] for the purposes of explaining "why registration is important for UNHCR and its partners"; "how the registration system is intended to ensure that each individual and each household will have an accurate and lasting record, a means of identifying themselves, and a full and equitable share of benefits"; and "the rights, obligations and benefits that come with registering and the consequences of failing to register."[288] Judging from UNHCR's experience in Pakistan, open dialogue and education has proven effective in building support for, or at least acquiescence to, fingerprinting.

---

people—even totally innocent people—have no legitimate expectation of privacy in their fingerprints, and that's that."). *But see* Goetz, Fingerprinting under Scrutiny, *supra* note 134 (quoting a New York City resident, who was fingerprinted as a condition of her receipt of public assistance: "I'm a U.S. citizen, born and raised in the Bronx all my life. I have my identity in the health department and Social Security. And yet I'm being treated like a criminal.").

285. "'In Japan, fingerprinting has been limited to those arrested for crimes, so treating foreigners the same way [as criminals] is a serious human rights violation,' said Mitsuru Namba, a lawyer at the Japan Federation of Lawyers Associations." Yoko Kubota, *Japan Fingerprints Foreigners as Anti-Terror Move*, Reuters, Nov. 20, 2007, *available at* http://www.reuters.com/article/idUST23858020071120.

286. Article 6(3) provides, in part: "An alien who seeks to apply for landing as set forth in the preceding paragraph shall provide to an immigration inspector information for personal identification (fingerprints, photographs or other information . . . that serves to identify the individual. . . .) in an electromagnetic form. . . ." (Act No. 319 of 1951) Shutsunyukokukanri oyobi Nanminninteiho no ichibu wo kaiseisuru horitsu [Immigration Control and Refugee Recognition Act], Law No. 73 of 2004, art. 6(2).

287. UNHCR Handbook for Registration, *supra* note 147, at 86.

288. *Id.* at 87.

IV. CONCLUSION

Although the application of biometrics to refugees and asylum seekers is a relatively recent development, it has markedly improved national and international efforts to promote their welfare. The impact of biometrics has been felt directly, such as in refugee camps or through programs designed to reduce the incidence of detention, and indirectly, such as by addressing fraud and security concerns and thereby improving the political viability of efforts to protect refugees and asylum seekers. Although biometric technology is not free from misuse, there exist safeguards that are to some extent responsive to unique concerns of refugees and asylum seekers. To the extent that these safeguards can be improved and expanded upon, biometrics will continue to be an important tool in protecting refugees and asylum seekers.