IRAP
International Refugee Assistance Project

Extreme Refugee Vetting: FBI Bulk Communications Matching

Summary:
Through discovery in its lawsuit *Doe v. Mayorkas*, IRAP learned that since 2016, the FBI has been using a discredited bulk communications matching technique to vet and reject refugees from a list of predominantly Muslim-majority countries, leading to a steep, unfair increase in security denials.[1]

Background:
In 2018, the International Refugee Assistance Project ("IRAP") filed a lawsuit challenging the mass denial of refugee admission to dozens of Iranians of minority religious faiths with family in the United States. The refugees had been invited by the U.S. government to leave Iran and transit through Vienna, Austria to complete their refugee applications in a safe location under the Lautenberg Program. Congress created the Lautenberg Program in 1989 to facilitate refugee admission of persecuted religious minorities and other vulnerable groups from certain countries, including Iran, by lowering some eligibility restrictions and mandating certain procedural protections.

Through discovery in the lawsuit, IRAP learned that in 2016 the U.S. government implemented a radical change to refugee security vetting without notice to the public: The State Department and the Department of Homeland Security implemented the FBI proposal to use a discredited bulk communications matching technique to vet and reject refugees from a list of predominantly Muslim-majority countries.

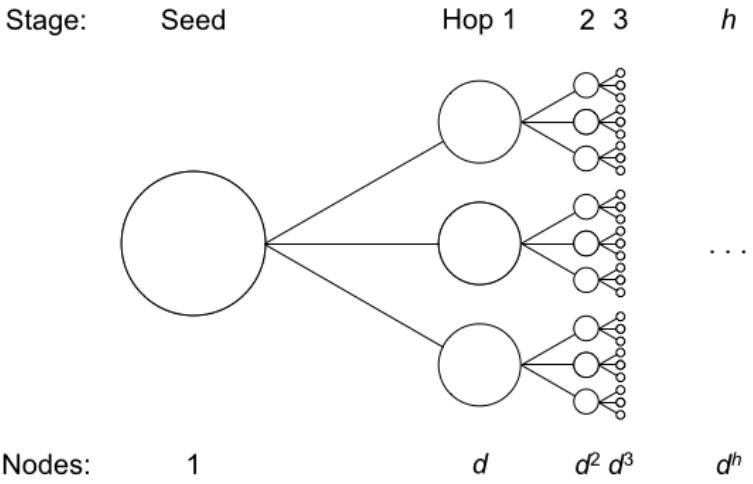
➡ **The use of bulk communications matching in refugee vetting caused a large jump in denials of refugees who became caught up in the U.S. mass surveillance capabilities for entirely innocent reasons.**

What is Bulk Communications Matching?
The most prominent and publicly known example of the use of bulk communications matching by the U.S. government is the controversial telephone surveillance technique first revealed to the public by Edward J. Snowden, who disclosed that the National Security Agency ("NSA") was analyzing a bulk database of telephone records of every American. When the NSA was investigating a person of interest, it would search the database to identify all phone numbers that had made or received calls from the target person's phone ("one hop"), all numbers that had made or received calls from the one-hop number ("two hops"), and all numbers that had made or received calls from the two-hop number ("three hops").

[1] For more detail, see International Refugee Assistance Project, Debunking "Extreme Vetting": Recommendations to Build Back the U.S. Refugee Admissions Program at 43 (revised June 2021), *available at* https://refugeerights.org/wp-content/uploads/2021/06/Vetting-Report-2020-v6-REVISED-JUNE-2021.pdf; International Refugee Assistance Project, Doe v. Wolf: Challenging the mass denials of refugee status to Iranian religious minorities, *available at* https://refugeerights.org/news-resources/doe-v-nielsen-challenging-the-mass-denial-of-refugee-status-to-iranian-religious-minorities

IRAP
International Refugee Assistance Project

Even though Congress ended the NSA program in 2015 following public outcry, the law still allows U.S. government agencies to collect telephone records of people, including Americans, who are within two hops of a person of interest. Under this two-hop collection, the government has amassed millions of records of entirely innocent phone calls; for example, it could collect call records of people who inadvertently received the same unwanted spam call as a person of interest.



This graphic of the NSA program by Jonathan Mayer shows that even if each caller were to call only three people, the relationship is attenuated between each hop and the number of people within 2 and 3 hops of the original caller becomes exponentially high.

How Is Bulk Communications Matching Used in Refugee Vetting?

IRAP's findings in *Doe v. Mayorkas* are the first evidence that controversial bulk communications matching techniques are being used to trigger rejections of refugee applicants.

Refugees are required to share a large amount of personal information with the U.S. government in their applications, including any phone numbers and email addresses that they have used for the past 10 years, as well as contact information of people in the United States—often family members—with whom they intend to reunite. Plaintiffs believe that the FBI vetted this information and automatically labeled as a security threat any refugee whose communication records matched with those in the government's vast bulk database, even though the database includes records of entirely innocent people caught up in the U.S. government's mass surveillance capabilities.

Who the Vetting Change Applies to:
This refugee vetting change applies to refugees ages 14 to 50 who are from countries on the Security Advisory Opinion ("SAO") list, which has been publicly reported as of October 2017 to be: Egypt, Iran, Iraq, Libya, Mali, North Korea, Somalia, South Sudan, Sudan, Syria, and Yemen.[2]

Key Sources: Appendix to Debunking "Extreme Vetting"[3]

- Exhibit 3(a): Summary of Conclusions, SAO RRB – Nov. 10, 2015 (*Doe v. Wolf*, DEF-13914)
- Exhibit 4: Emails re FTTTF – July 30, 2018 (*Doe v. Wolf*, DEF-143)
- Exhibit 37: Summary of Conclusions, SPCC – Apr. 16, 2018 (*Doe v. Wolf*, DEF-10250)

[2] SAO checks are also required for certain stateless Palestinians, those who are flagged as a result of a CLASS check, or refugees who are specifically flagged by PRM or USCIS.
[3] Available at https://refugeerights.org/news-resources/debunking-extreme-vetting-recommendations-to-build-back-the-u-s-refugee-admissions-program.