Safeguarding the Online Presence of LGBTIQ Refugees

Team Members:
Brett Foster
Jenna Galli
Matthew O'Donnell
Alexander Puhalski

Advisors:
Fabio Carrera
Daniel DiMassa

Sponsored By:

ORAM
Organization for Refuge,
Asylum & Migration

Abstract

This project aided the Organization for Refuge, Asylum, and Migration (ORAM), located in Berlin, Germany, in developing safe practices used to sustain a web-based tool that assists LGBTIQ asylum seekers. We proposed changes for ORAM's web application and produced a guide that ORAM can use to educate refugees and asylum seekers on protecting their digital data. We also conducted interviews with experts in cybersecurity, data storage, or IT to identify security measures and services for ORAM to safely collect and store refugees' data. ORAM can use these recommendations to serve itself and its clients.

Executive Summary

The total number of displaced people worldwide has almost doubled over the past decade from 43.3 million people in 2009 to 79.5 million in 2019—the largest number ever recorded (UNHCR, 2020a). Over 30 million of these refugees have been forced to leave their country of origin and are displaced abroad. Though many of these refugees are forced out due to conflicts and wars in their countries, others flee due to persecution. For example, of the almost 30 thousand asylum applicants in the UK in 2014, over one thousand (4.5%) cited their sexuality as a reason for fleeing (Pink News, 2017; Refugee Council, 2020). LGBTIQ individuals face discrimination and stigmatization globally. In 69 countries, same-sex relationships are even criminalized, and 6 of these countries include the death penalty as a punishment for these acts (Paletta, 2020).

To combat the persecution that LGBTIQ individuals face worldwide, the **Organization for Refuge, Asylum & Migration (ORAM)** provides guidance for LGBTIQ refugees navigating the asylum process. ORAM protects refugees through legal representation and conducts research investigating the challenges that these groups face (ORAM, 2021). ORAM has a web application, seen below, through which it provides a direct helpline for refugees, referrals to LGBTIQ-safe organizations, and information on asylum procedures. This app, which was created by a previous WPI student group in 2020, also enables ORAM and its external

ORAM's Web App Seen from a Desktop View

stakeholders to gather reliable data on displaced LGBTIQ persons in order to better research and assist these vulnerable populations (Alvarado et al., 2020). ORAM does not currently store the user inputted data. It does store the resources shown on the app in a Firebase database.

Although ORAM's web app is helpful for refugees to get the assistance they need, it can also pose a danger to its users. In countries where being LGBTIQ is criminalized, these individuals are forced to hide their identity, or else they are put in danger of being arrested or even killed. Similarly, the organizations in these countries that support the LGBTIQ community need to stay hidden, or their staff and the people they help could face similar threats. To protect these groups from being exposed, any data gathered by ORAM through its web app needs to be secure, to make it safe for individuals to access the application.

This project assisted ORAM in developing a secure web presence by proposing safe practices that it could implement in the web app to limit the potential dangers posed to its users. Our team **first** identified obstacles refugee groups face when accessing technology. We **surveyed refugees** who were in contact with ORAM and the LGBT Asylum Task Force (Worcester, MA) to obtain information related to the refugees' individual experience with technology and the participants' level of digital security knowledge.

Our **second** objective evaluated ORAM's interaction with refugees and asylum seekers to determine improvements for its web app. To obtain ORAM's refugees' perspectives on its web application, our team added a unique section to the ORAM refugee survey which focused on the experience refugees have had with ORAM's web app. From the survey responses, our team proposed a set of recommended changes for ORAM's web application and produced a guide that ORAM can use to educate refugees and asylum seekers on protecting their digital data.

Between both the LGBT Asylum Task Force and ORAM refugee surveys there were **13 responses**. Our team identified three security measure categories refugees should be trained on: **Wi-Fi, Passwords, and Social Media**. Seen on the next page is an infographic that could appear when accessing ORAM's application so that any asylum seeker can learn about personal security measures they can adopt to keep their digital data secure. Shown in Appendix G of the report, we created training materials that describe additional techniques, services, and tips LGBTIQ refugees can use to keep their personal data safe. ORAM, or any organization, can use the resources in the training materials to create informative curriculums for refugees.

Of the six respondents to the ORAM refugee survey, five answered the last part of the survey relating to ORAM's web application. A **majority** of refugees stated they were aware of ORAM's web application, but **none** had used it before. This may be due to the respondents

previously contacting ORAM before this application was created, and therefore, they had no reason to use the application. A majority of respondents requested **more languages** with one respondent asking for Swahili. The current web application includes three languages: English, French, and Spanish. Adding languages to the web application can be a slow process that ORAM can work on, starting with adding some common languages among asylum seekers. Additionally, refugees requested some form of better **communication via email**. Our team analyzed these responses by focusing on ways to improve the communication side of the web application.

Overall, our team recommends ORAM make the web application a staple of its home page. In addition, the web application should include some form of contact information for either ORAM to get in contact with the asylum seekers or the asylum seekers to get in contact with ORAM. The best option would be to include both. Currently ORAM has an additional comments section on the web application (as shown previously in the figure depicting ORAM's web app from a desktop view), but responses are not being stored. Therefore, any additional comments will not be seen by a representative at ORAM. Our team recommends the removal of this section from the web application. Once ORAM starts collecting information, there will still not be a

Refugee Security Measures

ORAM

REFUGEE SECURITY MEASURES

Tips refugees can use to keep their personal data secure

WIFI

Verify the WiFi **network name**
  o FreeAirportWifi vs FreeairportWifi

Only visit websites with **HTTPS encryption**

Use a **VPN** (virtual private network)

Disable bluetooth when using public WiFi

PASSWORDS

Use **logical groups** to organize passwords
  o different passwords for social media and financial institutions

Use **passphrases** instead of passwords
  o "This is my super secure password 90#" can turn into TimSsP90#

Use **password managers**

Use **multi-factor authentication**

No PIN numbers, addresses, or birthdays in passwords

SOCIAL MEDIA

Don't overshare

Use an **alias**

Don't post identifying features

Avoid giving **personal information** to someone who calls, emails, or texts

need for the additional comments section because refugees can instead use ORAM's email to reach out to the organization. Additionally, through the ORAM survey responses, our team identified the need for the web app to adopt additional languages. ORAM has also expressed the desire to collect the country the refugee is attempting to retreat to, identity of the refugee, and if there is more than one person who needs help. By combining ORAM's and its clients requests we created a mock web application, seen below, with the recommended features and changes.

Recommended Design for ORAM's Web App From a Mobile View
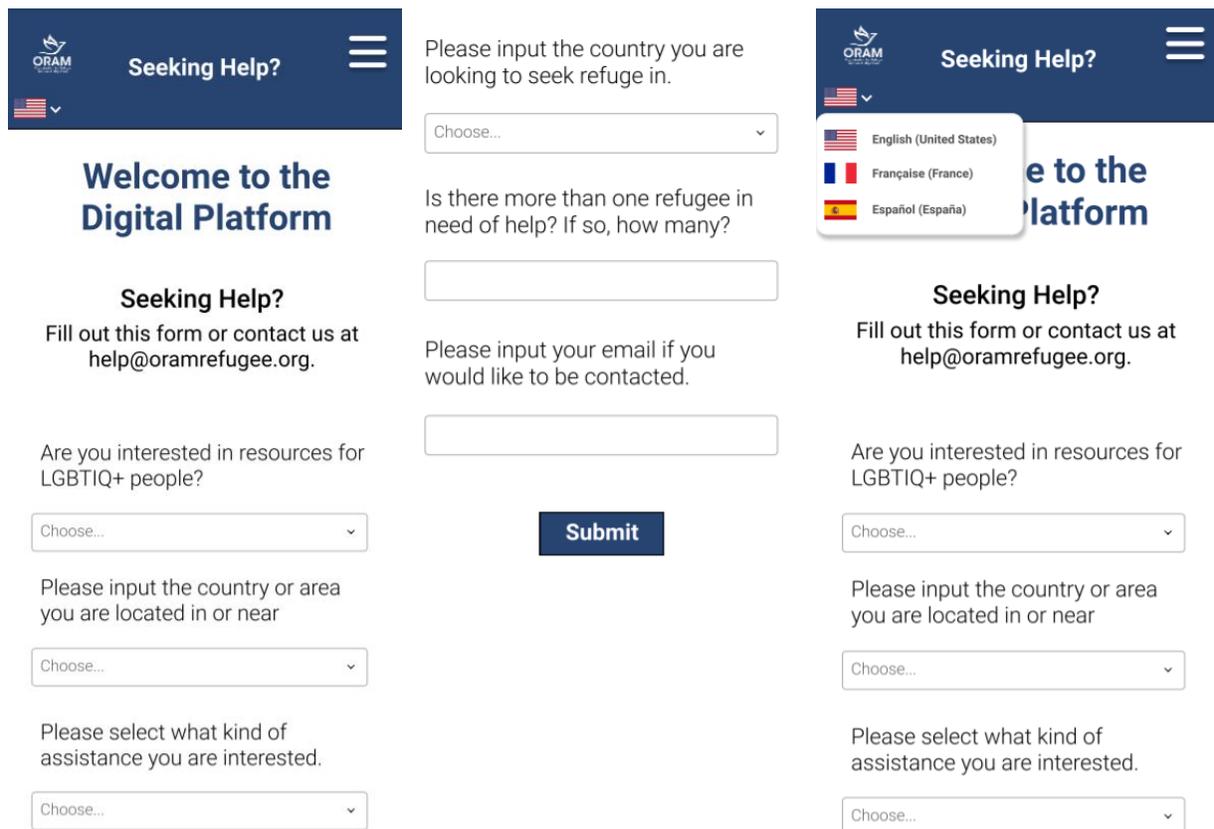
Finally, our **third** objective determined security measures and data collection methods that ORAM could adopt to keep its online applications safe. To identify potential security recommendations, our team **interviewed WPI Faculty** with a background in data storage, cybersecurity, or information technology (IT). Our team also **interviewed ORAM's IT volunteer** to discuss the feasibility of the recommendations we received from the faculty interviews. We then gave each security measure a quantitative score on a scale of one to three, from worst to best, for affordability, ease of use, and security, to determine which ones would work best for ORAM.

In order to gain a more detailed understanding of the issues and concerns we were trying to address, our team conducted a series of five interviews with faculty and staff at Worcester Polytechnic Institute and one interview with ORAM's IT volunteer. It became clear as we conducted more interviews that the **safest data is the data that is not collected**, so only ask users for what is absolutely necessary and can be justified. One of the most effective ways to secure any collected data is through **encryption**. Using an existing encryption service that adheres to ISO 27000, the international security standard, will be more than sufficient for ORAM. Another major takeaway from these interviews concerned the storage of sensitive data. There was a mix of opinions on the pros and cons of online versus offline databases, but the general consensus was that **if data is encrypted locally, it can be stored safely online**.

After identifying and analyzing a list of possible security measures and services that ORAM could use to better protect its data, we narrowed the list down to determine which options were most suited for ORAM's needs. Out of all the encryption services we analyzed, **the option with the best combination of security, ease of use, and price is Microsoft Office's "Encrypt with Password" feature**, which can be used to encrypt any Word, Excel, or PowerPoint file. If ORAM needs to encrypt any non-Office files, then the next best option would be to use Cryptomator. As long as sensitive documents are encrypted locally, they can be safely stored in any mainstream cloud storage service, but based on our evaluation **we recommend that ORAM uses either Google Drive or Microsoft OneDrive**. Further security recommendations we had for ORAM include:

1. Using strict access controls
2. Pseudonymizing personal data
3. Expanding its IT staff in the future

Table of Contents

List of Tables

List of Figures

Authorship

The authors of this report are Brett Foster, Jenna Galli, Matthew O'Donnell, and Alexander Puhalski. Each member of our team contributed equally to this report. Chapters and objectives were divided and distributed to each team member. When a section was written, each of us critically edited it to ensure the ideas expressed in the section were representative of what our team wanted to present. Furthermore, Professor Carrera, Professor DiMassa, and Professor Foo contributed to the editing and revision of the report throughout the process.

Brett Foster was a primary author of:
>Introduction
>Background Sections: 2.1, 2.1.1, 2.1.2, 2.3.2
>Methodology Sections: 3.3.1, 3.3.3
>Results and Analysis Section: 4.3.1, 4.3.2, 4.3.3, 4.3.4
>Conclusions and Recommendations Section: all of 5.3
>Appendices A, D, E, F
>The team's website

Jenna Galli was a primary author of:
>Executive Summary
>Background Sections: 2.2.3, 2.2.4, 2.3.1
>Methodology Section: all of 3.1
>Results and Analysis Section: all of 4.1
>Conclusions and Recommendations Section: 5.1
>Appendices: A, B, C, F, G

Matthew O'Donnell was a primary author of:
>Background Sections: 2.2, 2.2.1, 2.2.2
>Methodology Section: all of 3.2
>Results and Analysis Section: all of 4.2
>Conclusions and Recommendations Section: all of 5.2
>Appendices: A, B, F

Alexander Puhalski was a primary author of:
>Abstract
>Introduction
>Background Sections: 2.1.3, 2.1.4, 2.3.2
>Methodology Sections: all of 3.3
>Results and Analysis Sections: 4.3.1, 4.3.2, 4.3.5
>Conclusion and Recommendations Section: all of 5.3
>Appendices: A, D, E, F

Acknowledgements

1. Introduction

The total number of displaced people worldwide has almost doubled over the past decade from 43.3 million people in 2009 to 79.5 million in 2019—the largest number ever recorded (UNHCR, 2020a). Over 30 million of these refugees have been forced to leave their country of origin and are displaced abroad. Though many of these refugees are forced out due to conflicts and wars in their countries, others flee due to persecution. Of the almost 30 thousand asylum applicants in the UK in 2014, for example, over one thousand (4.5%) cited their sexuality as a reason for fleeing (Pink News, 2017; Refugee Council, 2020). LGBTIQ[1] individuals face discrimination and stigmatization globally. 42 UN member states have legal barriers to expression of LGBT identity, and 51 member states have legal barriers preventing non-governmental organizations (NGOs) from working on issues related to sexual and gender diversity (Paletta, 2020). In 69 countries, same-sex relationships are even criminalized, and 6 of these countries include the death penalty as a punishment for these acts (Paletta, 2020).

In comparison with many other Western European countries, Germany stands out for its progressive immigration and refugee policy. Unlike most other nations that are members of the European Union, Germany has welcomed large numbers of refugees with a hope that doing so could boost economic growth. Starting around 2015, Germany began following a '*Willkommenspolitik*' or 'Welcome Politics' approach to admitting refugees (Soederberg, 2019). This practice notably contravened the EU Dublin III Agreement which required all refugees entering the EU to apply for asylum with the first EU nation they set foot in (Funk, 2016). Germany began accepting asylum applications from refugees regardless of if they had previously been in another country where they could have sought asylum so long as the country of origin from which they were fleeing was deemed unsafe (Funk, 2016). In this manner, they could be granted protected refugee status or asylum for one to three years, but would be deported to the country they first set foot in if their reason for fleeing their home was not based on a legitimate fear for safety (Funk, 2016). This progressive approach led to a surge in refugees applying for asylum during the Syrian refugee crisis with 55,001 refugees entering Berlin in 2015 alone (Soederberg, 2019). Although these numbers have decreased in years since, Germany continues to be a country many refugees seek to enter. In addition to overall favorable asylum policy, German legislation regarding LGBTIQ rights has been generally ahead

---

[1] 'LGBTIQ' is an acronym for lesbian, gay, bisexual, transgender, intersex, and queer.

of other countries. Same sex partnership has been legal in the country since 2001 and marriage since 2017 (Jones, 2017). While there is still much debate and division within the country on many aspects of LGBTIQ rights, altogether progressive laws on sexuality make Germany an even more viable option to LGBTIQ refugees seeking asylum because of their sexual orientation.

To combat the persecution that LGBTIQ individuals face worldwide, the **Organization for Refuge, Asylum & Migration (ORAM)** was formed in 2008, and its European office is currently based in Berlin, Germany (ORAM, 2021). ORAM is an independent, nonprofit NGO that provides guidance for LGBTIQ refugees navigating the asylum process, protects refugees through legal representation, and conducts research investigating the challenges that these groups face (ORAM, 2021). One of ORAM's current projects to achieve these goals is a web application through which it provides a direct helpline for refugees, referrals to LGBTIQ-safe organizations, information on asylum procedures, and a support community for LGBTIQ individuals. This app, which was created by a previous student group in 2020, also enables ORAM and its external stakeholders to gather reliable data on displaced LGBTIQ persons in order to better research and assist these vulnerable populations (Alvarado et al., 2020).

Although ORAM's web app is helpful for refugees to get the assistance they need, it can also pose a danger to its users. In countries where being LGBTIQ is criminalized, these individuals are forced to hide their identity, or else they are put in danger of being arrested or even killed. Similarly, the organizations in these countries that support the LGBTIQ community need to stay hidden, or their staff and the people they help could face similar threats. To protect these groups from being exposed, it is imperative that any data gathered by ORAM through its web app is kept secure, and that it is safe for individuals to access the application.

This project aided ORAM in developing a secure web presence by proposing safe practices that it could implement in the web app to limit the dangers posed to its users. We identified obstacles LGBTIQ refugee groups face when accessing technology in order to provide them specialized security measures to protect their data. Next, we evaluated ORAM's interaction with refugees and asylum seekers in order to determine improvements for its web app. Finally, we recommended security and data collection methods for the web application that ORAM can adopt to keep its users safe.

2. Background

In 2015, at the height of the European migration crisis, asylum seekers and European governments faced unprecedented challenges. These governments followed different protocols to address the crisis, but Germany's procedures stood out. The arrival of so many refugees between 2015 and 2018 caused Germany's socio-economic practices to change drastically (Azizi, 2018). Its asylum process endured enormous strain and criticism. There are still legislative difficulties in the asylum process that may mentally drain asylum seekers, and some vulnerable populations continue to face obstacles even after settling into their host country.

LGBTIQ refugees experience an especially large number of obstacles throughout their asylum process. Many countries of origin for these vulnerable populations have implemented legislation opposing LGBTIQ individuals. In addition to such laws, asylum seekers can face threats if their incriminating personal information were to be exposed. In order to assist these vulnerable populations, many organizations, such as the Office of the United Nations High Commissioner for Refugees (UNHCR), work to protect refugees around the world. The Organization for Refuge, Asylum & Migration (ORAM) provides legal consultation and representation to asylum seekers and refugees. These organizations devote resources to advocating for these social issues, but asylum seekers and refugees still experience obstacles in communication.

Social media can have both a positive and negative impact on refugees and asylum seekers. Digital social communities allow refugees to adjust and settle into their new location. The use of technology allows refugees and asylum seekers to communicate with family and friends in their country of origin. This helps eliminate social isolation and leads to many positive effects. Unfortunately, due to the prevalent digital divide, asylum seekers face many factors that inhibit their access to technology, one of which is the lack of access to technological services. This has led to a deficit in online knowledge for refugees and asylum seekers and may have limited their understanding of data protection measures. This is a significant obstacle for these vulnerable populations especially since their safety resides in the ability to remain anonymous. Data protection is a crucial skill for refugees and asylum seekers to ensure their safety. By understanding the limitations of technology for refugees, deliverables can be produced around these obstacles.

2.1 European Refugees and the Asylum process

World War II generated the largest refugee crisis in European history prior to the 21st century (UNHCR, 2000). As the Nazis invaded countries throughout Europe, they sent millions of captured civilians and prisoners of war back to Germany, where they were used as slave laborers. Following the defeat of Nazi Germany, the 11.3 million foreign forced laborers that survived found themselves displaced (UNHCR, 2000). Another group that found themselves displaced from their home country at the end of the war were 13 million ethnic Germans who lived outside Germany's national borders (UNHCR, 2000). Many Germans resettled to live in the countries that the Nazis occupied and then either fled or were expelled after these countries were annexed by the Soviet Union and the Allies. Additionally, another 40 million people were displaced in Europe such as survivors of labor and concentration camps, groups expelled by and fleeing from Nazi Germany, and people who fled the advancing Soviet armies (UNHCR, 2000). In total, over 64 million people were displaced in Europe in May of 1945 following the collapse of Nazi Germany (UNHCR, 2000).

In order to tackle this global problem, the Allies set up the United Nations Relief and Rehabilitation Administration (UNRRA) in 1943, an international relief agency (UNHCR, 2000). Over the course of four years, the UNRRA repatriated approximately 7 to 8 million people (UNHCR, 2000). This mass repatriation was controversial, as many of the displaced people had no desire to return to their original country, such as East Europeans whose home countries were now under communist rule (UNHCR, 2000). For example, approximately 2 million Soviet citizens were quickly repatriated after the end of the war despite their objections, and many of them ended up in Stalin's labor camps (UNHCR, 2000). Due to the UNRRA's contentious actions, the United States stopped providing funding to them in 1947, and the UNRRA quickly ceased operations in Europe (UNHCR, 2000). The problem of mass displacement still existed, however, and so the International Refugee Organization (IRO), another United Nations agency, replaced the UNRRA in July of 1947 (UNHCR, 2000). Unlike the UNRRA, the IRO focused much more on the resettlement of displaced people to third countries, rather than on the repatriation of refugees (UNHCR, 2000). They were able to resettle over a million people during the few years they were active, though around 400,000 displaced persons still remained in Europe in 1951 (UNHCR, 2000). By this point, many of the IRO's responsibilities were handled by other agencies, for which reason its duties were taken over by the United Nations High Commissioner for Refugees (UNHCR), which still exists today.

Until this past decade, the displacement caused by the Second World War was the largest refugee crisis in history, but starting in 2015, a period known as the European Migrant

Crisis began (UNHCR, 2020a). By the end of 2019, a record level of **79.5 million people were displaced** from their homes worldwide, as shown in Figure 1, primarily in Syria, Iraq, Afghanistan, and other war-torn countries. In Syria, over 13 million civilians required assistance due to the civil war, 6.6 million were displaced from their homes internally, and 5.6 million fled to other countries (UNHCR, 2019). The European Union (EU) faced many challenges as a result. Though it originally accepted Syrian asylum seekers with open arms, the EU's policies proved to be ineffective and inefficient in providing for and redistributing the migrants (Fernández-Huertas Moraga & Rapoport, 2015). These obstacles forced the EU to reevaluate many of its policies such as the Dublin Regulation through which asylum seekers could only apply for aid in the member state that they first entered. Some EU countries temporarily rescinded the Dublin Regulation in order to receive additional refugees and more evenly distribute them across Europe (Fernández-Huertas Moraga & Rapoport, 2015). As a result of the refugee crisis, the EU now discourages migration within Europe and from countries considered "safe" (Fernández-Huertas Moraga & Rapoport, 2015). Although the peak of the European Migrant Crisis has passed, and some say that the crisis has concluded, the EU still receives many migrants and asylum seekers from these countries today.

Figure 1

Displaced Persons Worldwide by Year (UNHCR, 2020b; World Bank, 2019)
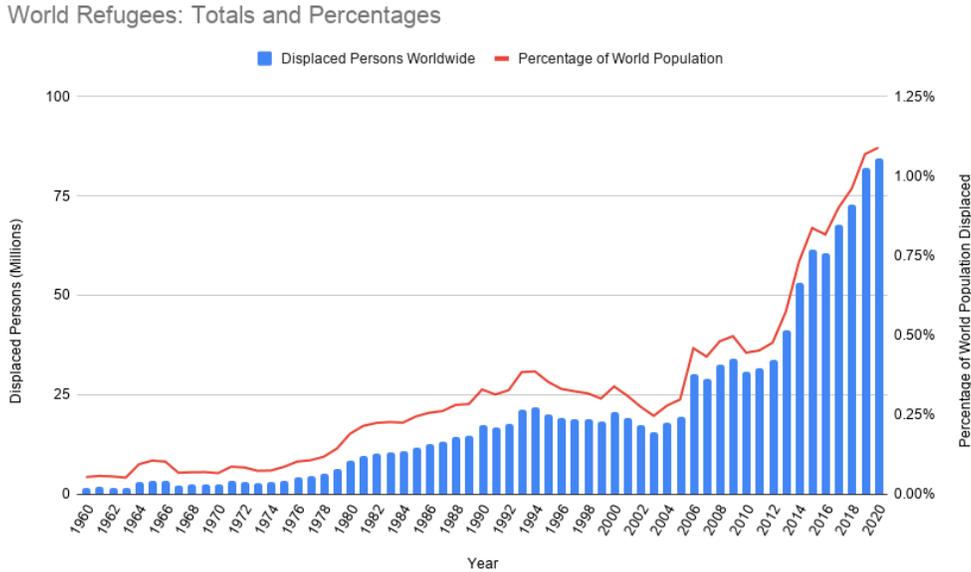
2.1.1 Refugee Routes into Europe

The policies and border control measures implemented by individual European countries often directly influenced the paths refugees took and their final destinations. From Syria, for example, there were numerous routes taken by refugees, such as west through Egypt and Libya to go across the Mediterranean Sea into Italy or Greece, or even further west to cross the Mediterranean into Spain, or an eastern path through Turkey and into Greece as seen in Figure 2 (Granados et al., 2016). Of these routes, Syrian refugees often chose the eastern path, known as the Balkan corridor, because of policies such as Spain's strengthened border control to limit smuggled migrants (Calka & Cahan, 2016). Similarly, most Syrian refugees gravitated towards lower risk countries with less border control, such as Turkey, Lebanon, and Germany (Calka & Cahan, 2016). Other policies had a significant impact on these paths, such as the 109-mile barrier built by Hungary along its southern border in 2015, which drastically decreased the number of migrants in Hungary but simply shifted the migrants' routes through nearby countries such as Slovenia, as seen in Figure 3 (Granados et al., 2016). Austria further slowed migration by passing legislation with the Balkan states to increase border control (Granados et al., 2016). This resulted in migrants being stuck in Greece at the closed Macedonian border (Granados et al., 2016). However, while most European countries passed legislation to slow the arrival of refugees, Germany stood out as one of the few countries actively helping refugees who entered the EU.

Figure 2

Routes Taken by Refugees (Calka & Cahan, 2016)

Figure 3

Impacts of Hungary's Border Fence (Granados et al., 2016)
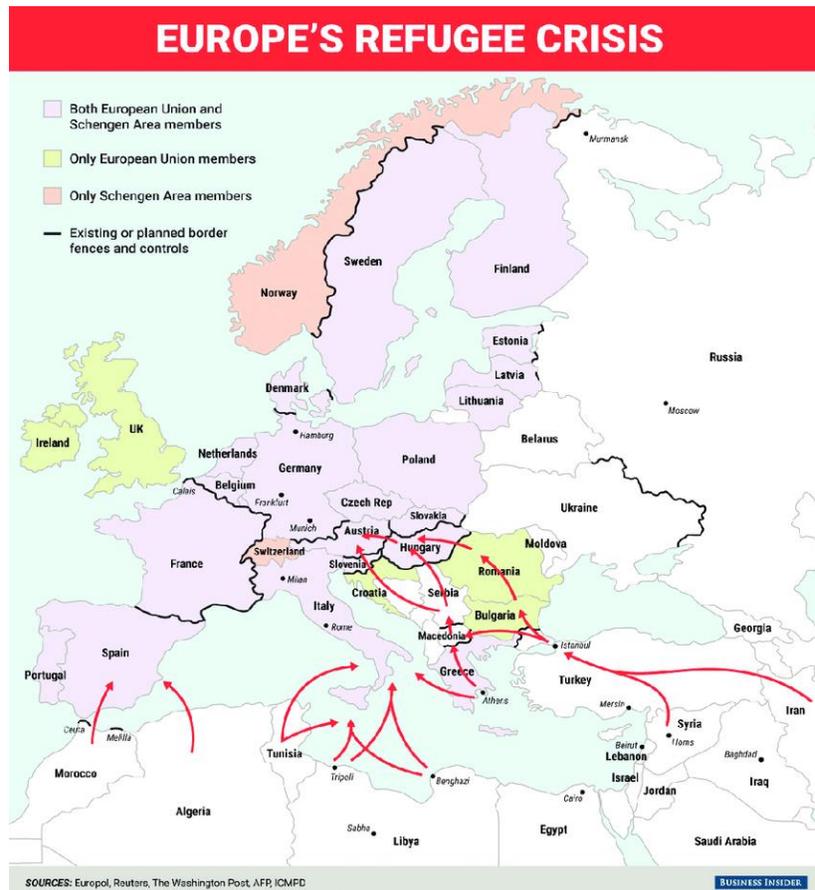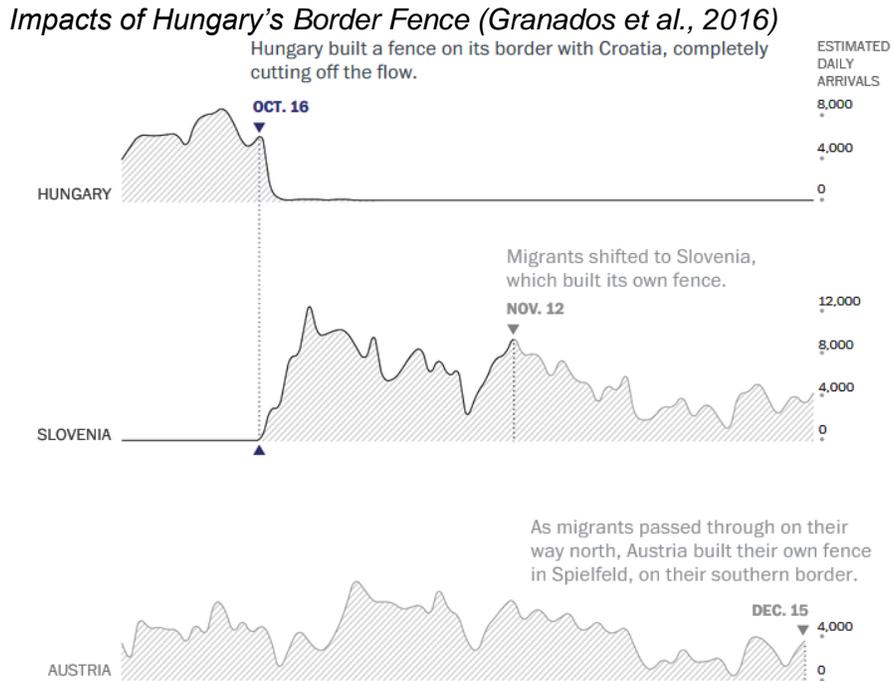
2.1.2 Refugees in Germany

As other EU countries attempted to close borders and stem the flow of migrants, Germany took a different approach and welcomed the refugees with open arms. It took in more asylum seekers than any other country in the EU with a total of 36 percent of the refugees, far ahead of the next closest countries, Hungary and Sweden, who accepted 13 and 12 percent of the refugees, respectively (Rietig & Müller, 2016). Even more refugees came to Germany after pictures appeared online showing Germans cheering for arriving refugees and Chancellor Angela Merkel taking selfies with refugees (Rietig & Müller, 2016). The spike of migrant arrivals can be seen clearly in Figure 4, which shows the number of refugees registered in Berlin by year.

This welcoming attitude towards refugees is also reflected in Germany's policies. At the peak of the Syrian refugee crisis, Chancellor Merkel suspended the EU's Dublin Regulation for Syrians, allowing their asylum applications to be processed in Germany even if they had passed through another European country first (Ayoub, 2019). Once the asylum seekers arrived in Germany, they also had access to hundreds of new volunteer initiatives offering short-term assistance and helping refugees gain a long-term foothold (Rietig & Müller, 2016).

However, while many Germans supported the refugees and Germany's migration

Figure 4

Berlin Refugees Graph With Marked Events (Alfred, 2016; International Rescue Committee, 2016; Knight, 2020; Soederberg, 2018)

Number of Refugees Registered in Berlin with Socio-Economic Events
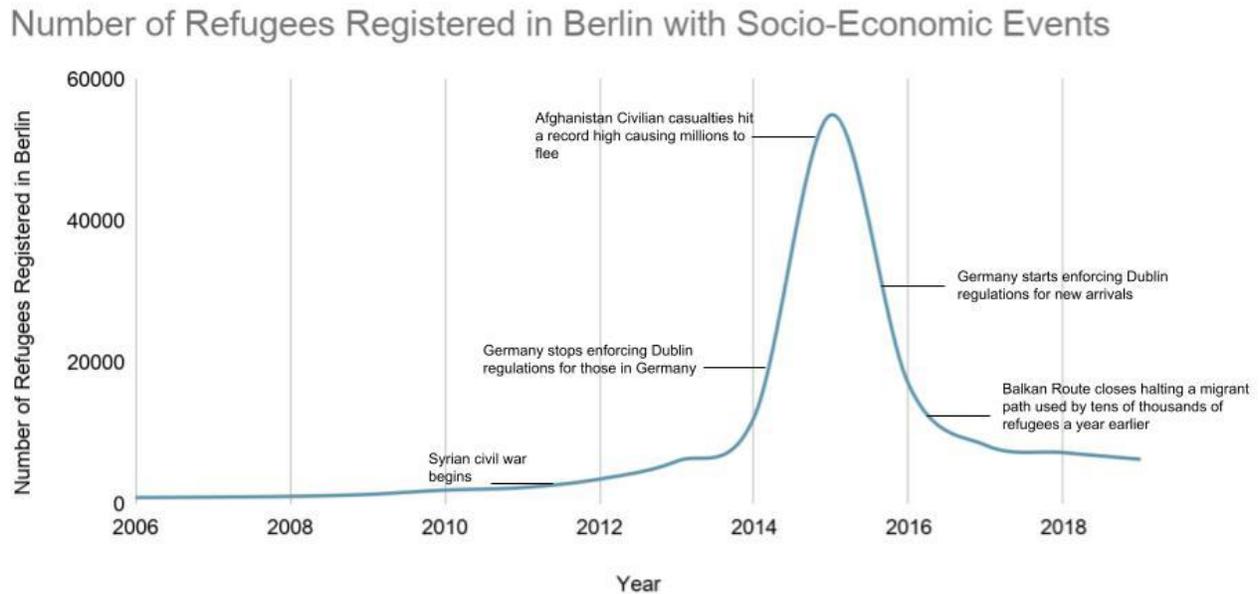
policies, many others displayed an anti-immigrant sentiment, and Merkel's popularity dropped from 75% in April 2015 to below 50% in February 2016 (Rietig & Müller, 2016). Although Germany's migration policies are more welcoming than those of other European countries, they do not mean that Germany provided unconditional support for refugees. The suspension of Dublin Regulation only applied to Syrians, and it was only temporary (Rietig & Müller, 2016). At the same time, Germany also introduced more border controls in September 2015 to restrict the number of refugees coming to Germany from Austria and the Balkan corridor, and it expanded the list of "safe" countries, whose migrants were likely to have their asylum applications rejected (Rietig & Müller, 2016). Despite this, Germany still remains one of the most popular destinations for people seeking asylum today.

2.1.3 Germany's Asylum Process

Germany's asylum process begins when an individual registers as an asylum seeker. This is done by contacting German authorities such as border patrol or an immigration office to complete an initial registration called '*Asylgesuch*' (Asylum Procedure, 2020). During this initial registration, the individual seeking asylum will be asked basic background questions and have fingerprints taken to be checked against other European countries. After this, asylum seekers must go through Germany's Federal Office for Migration and Refugees, the Bundesamt für

8

Migration und Flüchtlinge (BAMF), in order to submit an official application for asylum. Refugees are asked in-depth questions about their background and history. Once the application is complete, a temporary residency permit or "*Aufenthaltsgestattung*" is issued, which can serve as an official form of identification in Germany while the asylum process is carried out.

The next step in the asylum process is the so-called "Dublin examination". This is in accordance with the Dublin III Regulation, a cornerstone of the European asylum system meant to ensure that asylum seekers apply for asylum in the first country that they enter in which they are eligible (Hailbronner & Thym, 2016). If refugees are in another nation's system already, they may be sent back to the original country with that nation's permission (Asylum Process, 2019).

Assuming the Dublin examination is passed, a refugee's next step is to undergo an official hearing (Asylum Procedure, 2020). This can often be months after arriving but is a crucial component of the process. During the hearing, asylum seekers are asked to explain and talk in detail about their reasons for leaving their country of origin, how they got to Germany, and specifics regarding their life or experiences prior to seeking asylum. This hearing can be intimidating and stressful; many refugees must prepare and practice exhaustively to be ready. The goal is to ensure the refugee is eligible for asylum without any doubt.

Following the hearing, the asylum seeker will need to wait a few months before receiving a decision from BAMF. This can be one of five verdicts. They can be officially recognized as a refugee under the Geneva Refugee Convention[2], they can receive subsidiary protection, they can get a residence permit as a result of there being a ban on deportation, their application for asylum can be rejected, and finally it can be rejected as being 'obviously unfounded' (Asylum Procedure, 2020). If the individual is not satisfied with the decision, there are multiple legal avenues for appeal. The process is not easy and ultimately there are countless ways that a person's asylum application process can go wrong.

2.1.4 Difficulties in the Asylum Process

There is no doubt that the process one must go through to obtain asylum in practically every nation is a difficult and complicated one. Having entered the wrong country while trying to flee to somewhere else or having too many apparent inconsistencies throughout an interview process are just a few reasons a refugee might have their asylum application process derailed (Asylum Procedure, 2020). These difficulties can be complicated, and it can often be hard to

---

[2] Germany defines a refugee as an individual whose life or health is threatened because of an aspect of their identity (Asylum Process, 2019).

identify where something went wrong. Refugees trying to escape traumatic situations in their country of origin or fleeing for safety may find that the intensive asylum process is too much to handle by themselves. One study that examined the asylum process in the United States found **Post Traumatic Stress Disorder** or PTSD to be one of the major challenges faced by refugees seeking asylum (McVane, 2020). Common PTSD symptoms, such as finding it difficult to

recount relevant trauma and significant experiences, make it harder for refugees to defend why they should be considered eligible for asylum, and can even make their story appear inconsistent or fabricated when they are unable to recount certain details. Figure 5 depicts common health problems in refugees. The nature of the situations that drive people to seek asylum makes refugees more likely than a non-refugee to suffer from severe PTSD. This poses a major challenge for refugees in most countries' asylum processes.

Figure 5

Table of Common Health Problems Among Refugees (Mishori, 2017)

Table 5. Common Presenting Health Problems in Refugees

Mental health problems	Pain
Adjustment disorder	Abdominal pain
Anxiety	Headache
Depression	Musculoskeletal pain
Posttraumatic stress disorder	Pelvic pain in females
Sleep problems	**Undiagnosed chronic conditions**
Social isolation	Asthma
Nutritional problems	Chronic obstructive pulmonary disease
Anemia	Diabetes mellitus
Overweight/obesity	Dyslipidemia
Vitamin B_{12} deficiency	Hypertension
Vitamin D deficiency	Impaired fasting glucose levels
	Oral health problems

Adapted with permission from Eckstein B. Primary care for refugees. Am Fam Physi-cian. *2011;83(4):432.*

In Germany, even if asylum seekers suffering from PTSD or other mental health conditions sought medical help, they would find even more challenges in their path to receiving care. Asylum seekers have limited access to psychotherapeutic care due to the fact that despite their treatment not differing from the general German public, their corresponding costs associated with the care are not covered like they would be for German citizens (Nikendei, 2019). In a paper looking at how refugees' mental health develops throughout their experience with Germany's asylum process, it is stated that "Due to pre-, peri-, and post-migratory distress factors, fleeing people are at high risk of developing mental health problems" (Nikendei, 2019).

Germany's political landscape can present various difficulties as well. For some time now, different political parties have generally had vastly diverging views and opinions on immigration and asylum processes. This was exacerbated even more after the numerous arrivals of asylum seekers and refugees in Germany around 2016 and 2017 (Refugees, 2017).

The country's political parties became extremely opinionated on the current asylum process and proposed numerous different changes to asylum policy and practices. The far-right leaning nationalist party, known as Alternative für Deutschland (AfD), had the most stringent opinions during this time, calling for a zero-immigration policy and mass deportation of current refugees. They also explicitly opposed family reunification in the case of a zero-tolerance approach for refugees crossing German borders (Refugees, 2017). While the AfD's proposed policies ultimately were not turned into legislation, they serve to emphasize the volatility of political will regarding asylum. Whenever political power shifts in drastic ways, the chance of previously well-established laws and practices being modified or changed is high. For an asylum seeker, knowing that one's ability to apply for and receive asylum can change whenever power changes is a frightening prospect. Following the current asylum process is difficult enough as it is, and opposing political groups make it even harder.

2.2 Obstacles Faced by LGBTIQ Refugees

Refugees face many obstacles when attempting to seek asylum in a host country. They are threatened with persecution, death, rape, and more. Being an LGBTIQ refugee brings complications that make this process more difficult than it already is because of legislation opposing LGBTIQ individuals in host countries. Currently, there are still numerous countries that have specific laws against LGBTIQ individuals. Upwards of 69 countries have national laws that **criminalize same-sex marriage**. An additional nine countries have national laws that **criminalize gender expression** (Human Rights Watch, 2020). Figures 6 and 7 illustrate the countries with laws restricting LGBTIQ individuals.

Figure 6

Types of Anti-LGBTIQ Laws (Human Rights Watch, 2020)
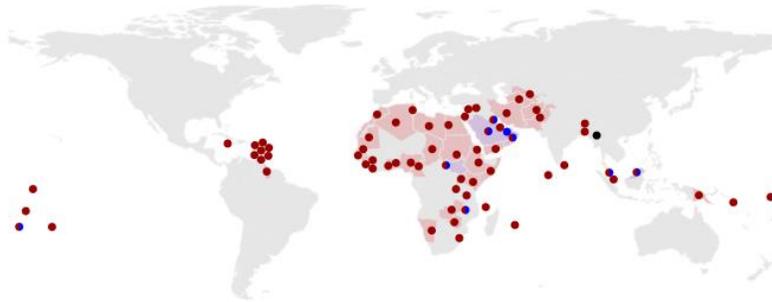
Figure 7

Laws Criminalizing Same-Sex Relations and Their Punishments (Human Rights Watch, 2020)
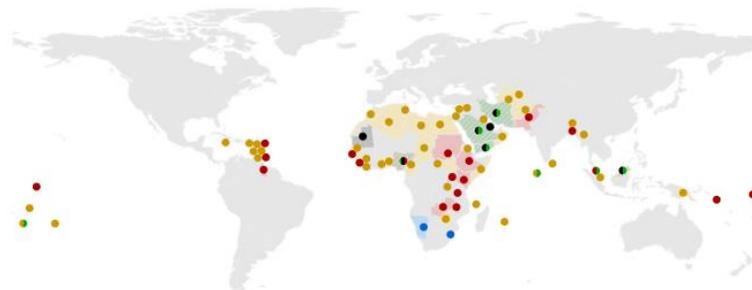
2.2.1 Legislation Opposing LGBTIQ Individuals

Many countries have legislation opposing legislation opposing LGBTIQ individuals, such as Cameroon, which outlaws all same-sex relations. The punishment for same-sex relations in Cameroon can be from six months to five years in prison with a fine of up to 200,000 CFA or $350 (Human Rights Watch, 2020). One story on the LGBT Asylum Task Force (Worcester, USA) website told by a man named Jean describes the horrors of being homosexual and living in Cameroon. While living in Cameroon, Jean concealed his sexuality by having a wife and kids. In 2005, the Cameroonian government discovered Jean had a secret boyfriend. Both of them were sent to jail and tortured, ultimately ending the life of Jean's boyfriend. Years later the Cameroonian government burned down Jeans Business and confiscated all his money. Once a wealthy man, Jean now lives in the USA with little to no money (LGBT Asylum Task Force, 2021). Unfortunately, Jean's story is not unique; it describes why many LGBTIQ individuals need to protect their identity until legislation allows for its safe expression.

2.2.2 Digital Threats Faced by Refugees

      Refugees face an enormous risk if their personal information is released to the government or public in their respective host country. LGBTIQ dating apps often play a significant role in exposing LGBTIQ individuals. There are numerous LGBTIQ friendly dating apps such as Grindr and Hornet. Grindr alone had over 27 million users by 2017 (BBC News, 2018). Additionally, global dating app usage has increased by 45% from 2015 to 2020 as seen in Figure 8 (Curry, 2019).

        Figure 8

       Global Dating App Users (Curry, 2019)

Global Dating App Users

Sources: IAC, MagicLab, Statista
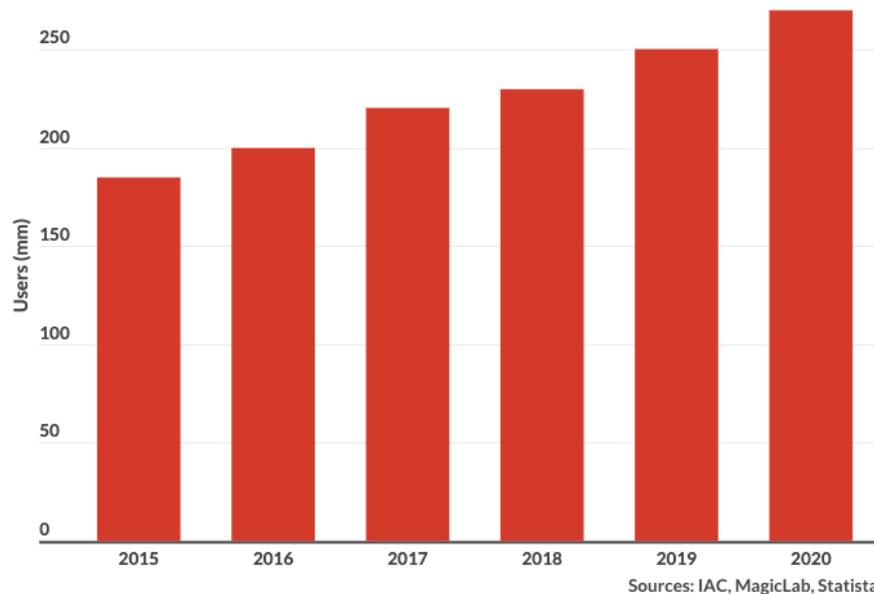
      These rising numbers are creating digital challenges for LGBTIQ refugees and asylum seekers. LGBTIQ refugees using these LGBT-friendly dating apps face the risk of being outed by a hateful person they meet online. This situation has happened before in Morocco where homosexuality is illegal. In 2020, Sofia Taloni, an Instagram influencer from Morocco, encouraged her 620,000 followers to download dating apps to out gay men (Al-Khal, 2020). Homosexual men in Morocco were then targeted on a dating apps by users who posed as potential dates. They were tricked into sharing intimate pictures of themselves with the people who were acting as potential partners. Once the malicious person acquired pictures, they leaked them online. Because homosexuality is illegal in Morocco, leaking these photos posed a serious threat to the LGBTIQ users' safety. Potential consequences included jail time, corporal

punishment, or even the death penalty. Grindr has acknowledged its role in these situations and has partnered with LGBTIQ activists to create the Holistic Security Guide (Grindr, 2019). This guide helps ensure the safety of its users by providing features such as blocking screenshotting for chats, pictures, and profiles. However, Grindr still acknowledges pictures can be captured from a second phone without the participant's consent. These threats are driving factors in the decision of LGBTIQ refugees to flee their country of origin.

Refugees continue to face threats even after settling into their host country. A study performed on 2,000 German citizens has shown that around three-quarters of them felt the increase of refugees to be a risk rather than an opportunity (Gerhards, 2016). In fact, the same study found that German citizens are less in favor of allowing refugees to seek refuge if their reasoning is the persecution of homosexuality or ethnicity. German citizens are less likely to support refugees who will undermine German culture and not abide by the social norms. LGBTIQ refugees could be treated poorly if the citizens around them knew their reasoning for fleeing. Securing this information from the public would allow LGBTIQ individuals to feel safer and more comfortable in their host country.

2.2.3 Worldwide LGBTIQ Humanitarian Organizations

There are a handful of humanitarian organizations that shield LGBTIQ individuals from persecution. The Office of the United Nations High Commissioner for Refugees (UNHCR) is one such organization dedicated to providing assistance to refugees around the world. Originally, the UNHCR was intended to be a temporary agency that assisted in the displacement of World War II refugees. However, a series of new conflicts, such as the Hungarian Revolution of 1956, led to the displacement of numerous people. This led to an ongoing need for the services of the UNHCR. Since then, the UNHCR has been a full-time service for refugees. The UNHCR has continued to work diligently to protect and assist refugees around the world throughout the decades (Hillstrom, 2018).

Some of the main resources the UNHCR provides are humanitarian relief and basic material assistance to refugees. This includes food, water, shelter, and medical care. In addition, the UNHCR provides various forms of services to assist refugees. Numerous refugees fleeing their country experience some form of trauma. The UNHCR provides psychological counseling services to help traumatized refugees once they are safe. One of the other main resources the UNHCR provides is legal protection. It ensures that refugees know their rights under international law and are given access to lawyers. The UNHCR will also talk to the host

governments to ensure that they are following all laws regarding the treatment of refugees (Hillstrom, 2018). This international organization is one of the leaders in providing refugee and migration assistance.

Another humanitarian organization that provides assistance to LGBTIQ refugees is our sponsor: **the Organization for Refuge, Asylum & Migration (ORAM)**. ORAM dedicates its resources to **providing legal assistance to LGBTIQ individuals** around the world who, because of their sexual orientation and/or gender identity, frequently face discrimination and severe violence in their home countries (Candid, 2021). LGBTIQ asylum seekers and refugees are often victims of bigotry, alienation, violence, and harassment. Rights and adequate protection for sexual and gender minorities (SGM) are not guaranteed in many countries. ORAM's mission revolves around establishing system-wide transformations through the use of innovative tools and pioneering research. Additionally, ORAM provides security to internationally displaced refugees by safely preserving confidential information in its systems. While ORAM was founded to advocate for SGMs, it has expanded its extensive programs to assist other highly vulnerable refugee communities in dire need of support. ORAM's mission of advocating for sexual and gender minority refugees fleeing violent environments has increased system-wide awareness and protection of vulnerable individuals (see Appendix A for sponsor description).

2.2.4 ORAM's Web Application

Prior to the year 2020, ORAM had an email helpline that it manually responded to, but in order to manage the influx of inquiries, the 2020 WPI-ORAM student team created a web application (Alvarado et al., 2020). Through this application, ORAM is able to **provide information to SGMs** regarding asylum procedures and LGBTIQ-friendly organizations in their country. Currently ORAM's web app, pictured in Figure 9, has three questions with a section for additional comments. The three questions inquire after LGBT status, location, and the kind of help needed. Once the questions are filled out and submitted, the web app will redirect the asylum seeker to local resources. This web app is also accessible through cellular devices, seen in Figure 10. ORAM does not currently store the user inputted data. It does store the resources shown on the app in a Firebase database.

Figure 9

ORAM's Web App Seen From a Desktop View (ORAM, 2021)

Figure 10

ORAM's Web App Seen From a Mobile View (ORAM, 2021)

The problem that arose from this web app is the ability to make it easily accessible for SGMs while simultaneously guaranteeing the safety of its users. By increasing the accessibility of its app, ORAM will be able to reach more LGBTIQ individuals and LGBTIQ-friendly organizations. However, this web app can also be dangerous for the organizations and people using it, as there are a number of countries in which being LGBTIQ is criminalized, and the exposure of user data can result in arrests or deaths. Because of this, **ORAM must make sure this information is secure** by implementing security measures. Through this application, ORAM dedicated its resources to improving and empowering the lives of endangered refugees.

2.3 Online Communication among Vulnerable Populations

During migration, virtual communities provide a sense of reliability while asylum seekers are separated from their home, relationships, and familiar environments. Scholars Jude Mikal and Braden Woodfield say the internet can be an effective communication tool for the transmission of advice, resources, and information while usual networks of support are unavailable (Mikal & Woodfield, 2015). Using focus group interviews, Mikal & Woodfield collected data about stress, social support, Internet technology, and connectivity. The four main questions asked during these focus group interviews discussed the transition to the United States, accessible technology in the United States, obstacles to accessing available technology, and upkeep of connections to the host culture. Findings show refugees use the Internet to maintain relationships within the target culture over large geographic distances. Furthermore, displaced populations use the Internet to find news about their country of origin and to research employment opportunities. The technological connection helps refugees adjust to their new lives and it aids asylum seekers in maintaining relationships thus partially mitigating the negative effects of stress migrants can experience. A Bletscher (2020) study, using descriptive surveys, focus groups, and interviews with refugees from three highly resettled metropolitan cities, focused on the level of refugee use of communication technologies, how refugees connect with sources of support, and the access to communication technologies for refugees. Communication technologies allowed better access to resources of support such as education and financial savings. Some disadvantages were mentioned by participants about technology usage such as new online "systems" were hard to interpret making navigation to apply for food stamps or a job extremely difficult. This is due to a multitude of factors, including physical access to technological resources, language, and transportation. While refugees and asylum seekers can benefit from both physical and virtual communities, a prevalent digital divide introduces some disadvantages to communication technology usage.

2.3.1 Refugee Access to Internet (Digital Divide)

Technology plays an important role for the over 80 million people who have been displaced since 2000, allowing them to maintain relationships, gather resources, and integrate into their new communities (UNHCR, 2020b). However, there are still uses, needs, and gaps to identify prior to utilizing technology to its full capacity. Alam and Imran (2015) explored factors influencing refugee migrants' adoption of technology and how it affects their social inclusion in Australia. Through a series of focus group discussions with refugees in Toowoomba,

Queensland, four key themes were identified as the motivator for digital inclusion and influencing of technical adoption. The four independent factors were **access, choice, affordability, and skills**. The article concluded that these obstacles were challenging the social inclusion of refugee migrant groups into the Australian community. For example, communication technologies were ineffective due to barriers related to language and skills to use the technology. Additionally, participants mentioned that the lack of broadband internet access adversely affected virtual school assignments, applying for jobs, and other e-services. Globally, 50 percent of refugees are less likely to have access to an internet capable phone than the general population (UNHCR, 2016). In addition, 20 percent of rural refugees have no access to connectivity while urban refugees usually cannot afford online connectivity. For some refugees, resettlement agencies or local libraries are their only access to technology, but inhibiting factors such as language and transportation limit this access (Bletscher, 2020). Gaps in connectivity have led to a knowledge divide between migrants who have skills and understanding of communication technologies and those who do not. When asked who they would consult about a broken device, participants responded that they did not know, they would try and fix it themselves, or "throw it away". While some of these responses are due to lack of financial resources, the others are from lack of technical knowledge.

Another contributing factor to the digital divide experienced by refugees and asylum seekers is age. Studies have shown children from early school age to young adults in their early twenties have a significantly higher familiarity with communication technologies (Bletscher, 2020). This lends itself to children becoming brokers of culture, language, and online knowledge on behalf of their parents (Mikal & Woodfield, 2015). In a study with Sudanese and Iraqi women, mothers often reported that their children were responsible for assisting them with online job applications. While this behavior is adopted by many immigrant children, the lack of language, culture, and technical learning will serve to intensify and prolong the dependency on their children. In this case, the internet does not eliminate stress for its users but rather it leaves parents unable to use the internet services and leaves children to explore the depths of the internet without any guidance. Since children are responsible for online activity, they are often left to independently explore and become victims of fraud. A lack of technological preparation for both adults and children leads to exploitation of sensitive data by authorities.

2.3.2 Exploitation of Data by Malicious Actors

Governments, authorities, and malicious groups all over the world have invested in gathering information on certain individuals online. One notable example of a government whose policies have led to widespread data exploitation comes from Lebanon. The Lebanese Constitution does not explicitly guarantee the right to privacy, and data protection laws adopted in 2018 are vague and inconsistent, leaving many important policies on individual data protection ineffective (Fatafta & Samaro, 2021). Not only do individuals lack the right to know how their personal data is used for national security, they are also unable to withdraw their consent to have their data collected. The Lebanese government has been known to give away their citizens' data, such as when they allowed certain security agencies unrestricted access to the electronic communications data of every citizen for a period of at least six months in 2014, and for another four months in 2017. In another case in 2018, the Lebanese Embassy in the UAE leaked an Excel spreadsheet containing the names, parents' names, date of birth, and addresses of over 5,000 Lebanese citizens. Another example of abuse by the Lebanese government pertains to two telecommunication companies that it owns called Alpha and Touch. These companies sold their users' data to outside groups or individuals for profit. This allowed businesses or anyone who purchased Lebanese citizens' personal data to do things like send emails or text messages to certain demographics based on gender, age, or even internet usage behavior.

In 2013, LGBTIQ activists were attacked by nationalist groups when protesting an early draft of the anti-gay "propaganda" law in Voronezh, Russia (License to Harm, 2014). This protest had been planned in advance, and the activist group had received approval from the municipal authorities to hold the gathering. When members of these nationalist groups learned about the planned protest through the activists' promotion of it online, they found and posted the full names, addresses, and social media accounts of the activists. The anti-LGBTIQ groups also urged their followers to "visit" the activists before their protest. Upon receival of death threats, members of the activist group went to the police to ask for action to be taken. The police suggested that the event be canceled. On the day of the protest, the dozen activists were faced by hundreds of counter protesters. When the attack started there were less than 30 police officers without riot gear who offered little to no help. Unfortunately, this is a reality for LGBTIQ individuals in Russia. Not only do they face threats from government opposition, but malicious groups target them as well.

Jordan, though well-intentioned, has exposed refugees to possible data exploitation risks. In 2016, the country installed a new iris scanning system in Azraq where around 30,000 Syrian refugees were housed (Staton, 2016). The iris scanning system reads the refugees' eyes, registers and stores the biometric data in the UNHCR database, and deducts their grocery bill from their monthly World Food Programme allowance. The system allowed over 600,000 Syrian refugees registered in Jordan to shop for food without the use of paperwork or cards. However, many refugees have experienced problems with the system. Since only the head of the household had access to the family's allowance, other friends and family members were unable to run errands on their behalf. This caused challenges for one refugee, Sabha, who was pregnant and worried she would not be able to obtain groceries as she entered her last trimester. Furthermore, there were dangerous risks associated with collecting biometric data. Since all the refugee data was stored in one UNHCR database, the prospective damage from cyber-attacks increased. This system is an example of how refugee organizations attempt to aid refugees, but instead place them in danger if their information were to ever be exposed. Since refugees are a particularly vulnerable population, there needs to be security measures to prevent organizations and governments from exploiting their data.

The risks LGBTIQ refugees face today from exploitation of data by malicious actors pose critical challenges that organizations like ORAM are trying to address. ORAM's web application has the potential to connect LGBTIQ individuals to the services ORAM provides, refer refugees to LGBTIQ-safe organizations, and provide information on asylum procedures. However, secure practices need to be utilized in order to ensure the safety of its users.

3. Methodology

This project was conducted to assist the Organization for Refuge, Asylum & Migration (ORAM) in the development of a secure web presence for LGBTIQ refugees. We researched safe practices that could be applied to online platforms to assist LGBTIQ individuals seeking asylum. We selectively identified relevant features and practices to protect the safety of LGBTIQ refugees and asylum seekers and proposed how to incorporate these best practices into ORAM's web site.

The primary objectives of this research project were:

1. To identify obstacles refugee groups face when accessing technology
2. To evaluate ORAM's interaction with refugees and asylum seekers
3. To determine security measures and data collection methods that ORAM can adopt to keep its online applications safe

Our project focuses on web app security for LGBTIQ asylum seekers and refugees. The refugees we contacted are limited to clients of ORAM and the LGBT Asylum Task Force (Worcester, MA). The LGBT Asylum Task Force is dedicated to supporting LGBTIQ individuals through providing resources such as clothing, housing, and food (LGBT Asylum Task Force, 2021). Figure 11 shows the relationship between our objectives, tasks, and final deliverables. The following sections describe the tasks we completed to achieve these objectives.

Figure 11

Methods Graphic
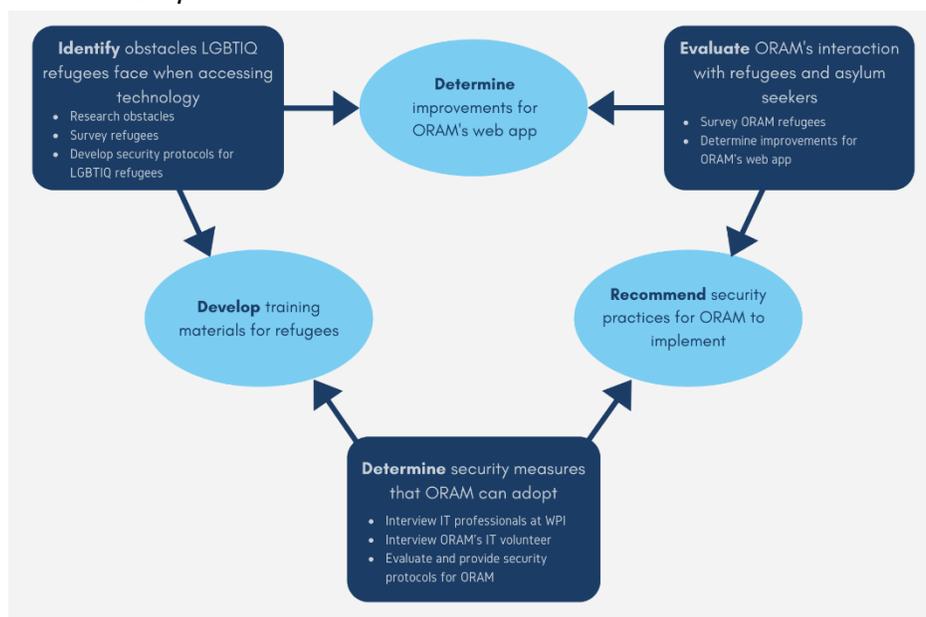
3.1 Identifying Challenges Faced by Refugee Groups When Accessing Technology

In order to determine obstacles refugees face when accessing technology, our team took a two-step approach. **First,** we conducted research to find **peer-reviewed articles** discussing refugee social media and dating app usage to understand their current security measures. In addition to these articles, our team also searched for sources giving recommended solutions for filling the technological literacy gaps caused by the digital divide. Finally, our team identified data protection strategies necessary for any internet user. For the **second** step in our approach, the questions that could not be answered through research were gathered and refined into a **survey** which was sent out to refugees.

3.1.1 Surveying ORAM and the LGBT Asylum Task Force Refugees

The refugees our team contacted were suggested by ORAM and the LGBT Asylum Task Force. These surveys were created with Google Forms. We sent **two separate surveys** to members of these organizations, and they contained many of the same questions. Figure 12 shows an overview of each survey's sections.

Figure 12

Overview of ORAM Refugee Survey and LGBT Asylum Task Force Refugee Survey
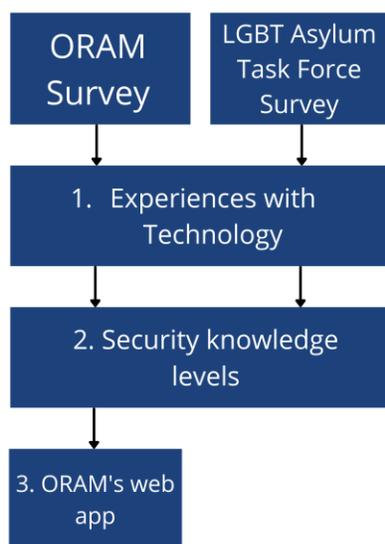
For both surveys, the first section's questions obtained information related to the refugees' individual **experience with technology** as well as their understanding of their community's experiences with those same technologies (see Appendix B and C for full survey questions), for example:

● If applicable, did you own the device you used to communicate with agencies, doctors, lawyers, or other asylum seekers during your asylum process?
● If applicable, during your journey, did you tend to use Wi-Fi or mobile data?
● To the best of your knowledge, is internet access readily available in the community in your first country of asylum?

The second section of questions in both surveys is related to the participants' level of **security knowledge**. One obstacle contributing to the digital divide is refugees' skills and knowledge levels of cyber security measures. By researching

data protection measures prior to this survey, our team based our survey questions off these measures. The survey responses identified which data protection measures refugees struggled to practice. This information assisted in creating infographics and training materials for refugees which will appear on ORAM's web application. Some questions in the surveys showed example images of emails and text message attempts of phishing as well as other perfectly safe texts and emails sent from companies. The participants who took the survey were asked if they would respond to that email or text which gaged their level of security awareness. Additional questions for this survey focused on password usage, social media, and the LGBTIQ community (see Appendix B for full survey questions), included:

- Do you use the same password for most things?
- How do you keep track of your passwords?
- Do you use phone numbers, addresses, birthdays, or other personally identifiable information in any of your passwords?
- If you use some form of social media, which platforms do you engage with?
- If you use some form of social media, do you engage with LGBT content on social media?
- If you use some form of social media, are you ever concerned about your data being public?

The last section of questions in the ORAM Refugee Survey will be discussed in the following section.

3.2 Evaluating ORAM's Interaction With Refugees and Asylum Seekers

When evaluating ORAM's interaction with refugees and asylum seekers, our team first looked into what information is relevant to ORAM and its stakeholders. ORAM stated they are looking to collect more personally identifying information with its web application.

Data ORAM wants to collect:
- Country refugee is attempting to retreat to
- Identity of refugee/asylum seeker
- Is there more than one person who needs help

Currently, the most relevant information to ORAM and its stakeholders is not being collected by the web app. In fact, there is no personally identifying data being collected. Since ORAM desires to include identities as a part of the form for the web application, we needed to suggest the proper improvements for the web application that will also protect refugees in the proper way. This leads into our next step which was **surveying** ORAM's refugees and obtaining their perspective on the web application. Our team utilized surveys because we wanted direct feedback from the refugees who would benefit from the app.

3.2.1 Surveying ORAM Refugees

In the ORAM refugee survey, our team included a third section focused on the experience refugees have had with ORAM's web application. These questions included:
- Is the web app easily accessible?
- If you have used the web app:
  - What features or aspects of it do you think were the most helpful to you?
  - What features would make the web app more helpful to you?
- What would you like to see in a web app that would have helped you with the asylum process?
- What additional information or services do you think ORAM could provide to help refugees seeking asylum?

The responses from the survey allowed us to suggest potential improvements to the web application (see Appendix B for full survey questions). Using this feedback, we provided recommendations to ORAM regarding what new features could be implemented in its web app to better serve refugees.

3.3 Determining Security and Data Collection Methods for ORAM's Application

ORAM intends to gather data on the refugees who use its app in order to conduct research and adapt its app to better serve its users. However, it needs to ensure that it collects data safely to avoid contributing to the vulnerability of these refugees. Similarly, ORAM suggests LGBTIQ-friendly organizations to the users of its web app. Since many of these organizations are located in countries where homosexuality is criminalized, it is important to ensure that these organizations are not put in danger by its information being revealed to the wrong groups. In order to provide ORAM with recommendations of security measures that it can implement, our team needed to understand what security practices are used throughout the industry. First, our team found the prevailing security measures in academia by reading peer-reviewed journal articles and researching the features of leading web apps. Then, in order to determine the appropriate security and data collection methods for ORAM's application, we followed three steps:

1. Interviewing WPI Faculty
2. Interviewing ORAM's IT Volunteer
3. Evaluating and Providing Security Protocols for ORAM

3.3.1 Interviewing WPI Faculty

After gaining a baseline knowledge of potential security recommendations, our team searched for faculty at WPI with a background in **data storage, cybersecurity, or information technology (IT)**. These faculty members would be able to provide us with more in-depth knowledge on the topics we researched as well as their personal opinions based on their experience in the field. Through a combination of getting recommendations from other WPI staff and through reading the faculty biographies on different department web pages, we identified a list of people we believed would be beneficial to interview. We sent emails to each of them explaining our project and why we were interested in talking with them. In the end, we conducted interviews with five people who had expertise in the fields of cybersecurity, data storage, and IT. Our team also interviewed an employee from the Diversity, Equity, and Inclusion staff to better comprehend the ethics presented from this problem. Some relevant questions from these interviews include:

- Can you provide us with a short background of your professional history and experience with work related to internet privacy and cybersecurity?
- What methods are generally used to track who uses a website, both by the owner of the website and by third parties
- Since ORAM is intending to start storing personal data from refugees, what methods might be feasible for this data storage? (A Google spreadsheet was utilized in the past, but we imagine this is not the most secure option.)
- If personally identifiable information (i.e. names, emails, etc.) are not being stored, is there still a risk of sensitive information (i.e. LGBTIQ status) being connected with the person who used the web-app
- We've done some research on ways to protect sensitive information and data encryption seems to be the most prevalent option. Do you have any knowledge on data encryption, and if so, do you know of any services that can be used for data encryption?
- Is there anything else you see as being important to address that we may be overlooking? Or any additional topics that you think could be worth reading up on?

See Appendix D for the complete list of interview questions. In order to get the most out of each interview, our team adjusted what we planned to discuss prior to each meeting based on the interviewee's background and experience.

By determining the most effective security measures being recommended by other industry professionals, our team identified what measures and practices ORAM could adopt in its own application to keep its users safe. This was done by putting all of the faculty interview responses in one document. Then as a team we highlighted repeated topics or questions that came up and labeled them as main takeaways to research further.

3.3.2 Interviewing ORAM's IT Volunteer

In order to understand what security measures would be feasible for ORAM to implement, we talked with the volunteer currently working on the information technology aspects of ORAM's web app. During the interview, we asked questions about prior work experience and knowledge of cyber security. We discussed what security measures have been implemented

and where the organization hopes to improve. Finally, we presented our main takeaways from our faculty interviews and asked the IT volunteer what would be feasible to implement for ORAM. To view the full set of questions asked during the interview, see Appendix E. Some relevant questions we asked include:

- Can you provide us with a short background of your professional history and experience working in IT, cyber security, and with ORAM?
- From your experience with the web app and email helpline, what do you see as being a potential security risk for ORAM? What is the way malicious groups would most likely try to exploit this data?
- Do you know if ORAM has ever been digitally compromised?
- Based on your experience with ORAM, do you think it would be wise for them to invest in more IT personnel to help manage and maintain higher security standards? What do you think would be the best way for them to go about expanding its investment in IT?
- In your opinion, what improvements if any does the web app need?

3.3.3 Evaluating and Providing Security Protocols for ORAM

Once we understood the current security standards in ORAM's web app and what the organization hoped to improve upon, the final step was to analyze the security measures we identified during our interviews with WPI faculty and IT staff to determine their **strengths, weaknesses, and feasibility** for ORAM. We conducted more in-depth research on each security measure to identify services offering these security protocols. Each service was ranked on three categories:

1. Affordability
2. Ease of use
3. Security

Table 1

Example Evaluation Matrix

Service	Affordability (/3)	Ease of Use (/3)	Security (/3)	Total (/9)

The rankings were done on a scale of one to three, from worst to best. Finally, the scores from each category were summed to give a quantitative ranking. The rankings for all the services were placed in a matrix, shown in Table 1, to easily compare them. The final set of security measures and best practices was presented to ORAM as part of our recommendations.

4. Results and Analysis

Through interviews with WPI faculty and IT professionals and surveys of refugees, our team collected valuable information. The following sections provide a summary of our key findings and an analysis of our results.

4.1 Obstacles Faced by LGBTIQ Refugees When Using Online Technologies

Between both the LGBT Asylum Task Force and ORAM refugee surveys there were **13 responses**. Of the 13 respondents, 10 (77%) described themselves as asylum seekers and 3 (23%) described themselves as refugees. Six respondents (46%) were between the ages of 25-30, three respondents (23%) were between the ages 30-50, three respondents (23%) were between the ages 20-25, and the last respondent (7%) was between the ages of 18-20. Nine respondents (69%) described an apartment as their current living situation, while 30% of participants said they live in a house and 7% of participants said they live in a safe house. Our team recognizes that having only 13 total responses to our survey is a limitation to how applicable our data will be to all refugees. We believe the low number of responses is correlated to the COVID-19 pandemic allocating other priorities besides our survey to refugees.

4.1.1 Half of Asylum Seekers Use Wi-Fi During the Asylum Process

Five out of thirteen respondents said they could not always rely on Wi-Fi during their journey as asylum seekers. In fact, two of the five said they strictly used mobile data. To receive mobile data, an individual would need to sign up for a phone plan, and this can be difficult for asylum seekers with unreliable finances. Without access to a stable internet connection, resources about the asylum process are challenging to locate. On the other hand, six respondents said they had access to Wi-Fi for the most part during their asylum process, and two of the six respondents said they strictly relied on Wi-Fi.

People with malicious intents will try to coerce individuals into logging onto their replicated public Wi-Fi network in order to steal personal data such as credit card numbers, passwords, emails, and photos. This **Wi-Fi hacking is dangerous** for refugees who may rely on public Wi-Fi not only at airports but cafes, train stations, and other public spaces. Since Wi-Fi poses a risk for refugees, our team presented tips for combatting Wi-Fi hacking (Appendix G).

4.1.2 The Vast Majority of Refugees Were Able to Recognize Phishing Attacks

        To aid refugees in risky situations involving personal data, our team collected information to evaluate refugees' knowledge levels relating to data protection. Our survey asked if the respondent would interact with an example email or text if it was sent to them. Figure 13 shows a phishing email from a university asking the user to click on a link to update their password.

Figure 13

Phishing Email #1 (Imperva, 2021)

        Ten respondents said they would not respond to the phishing email while two respondents said they would. One respondent said they would not respond because if the email had been sent from a real university, there would be actual names, departments, and contact information. Figure 14 shows another survey question with a real text message from the telephone provider AT&T asking to complete the set-up for a smartphone.

Figure 14

Real Text #1 (Grant, 2015)
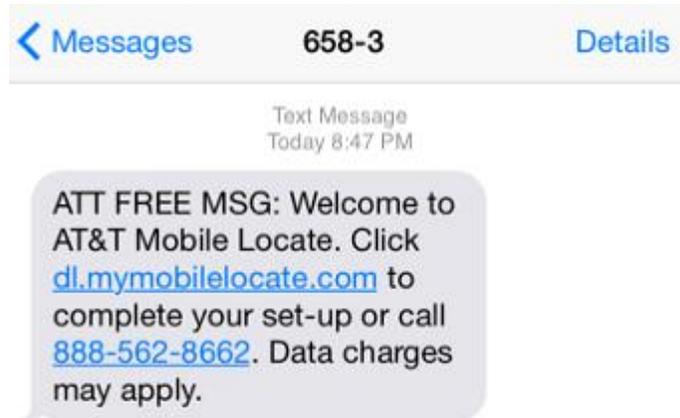
Eight respondents said they would not interact with this text because AT&T is not their service provider, and the URL is not associated with AT&T. Although this text was real, AT&T did use an outside provider for their URL. Organizations should be aware that using links that do not directly have their name in it will raise suspicion from the individuals interacting with the URL. From these responses, our team saw refugees and asylum seekers were **overly cautious when presented with possible phishing attacks.** Unfortunately, their caution did not extend to all hacker tactics.

After analyzing the responses from the refugee surveys, our team shifted our focus from protecting refugees from phishing attacks to providing security measures to protect their passwords. Three respondents said they used the same passwords for most websites, and two respondents admitted to using personally identifiable data, such as phone numbers, birthdays, and addresses, in their passwords. Additionally, three respondents physically write their passwords down, which may be acceptable for the average individual, but for LGBTIQ refugees who may be persecuted if their information is exposed, it is not the safest option. For example, if a family member finds an LGBTIQ individual's passwords, that relative could discover sensitive information they might not condone. By securing passwords, all accounts containing identifying data will be secured from the user side as well. Inadequate password security measures create avoidable risks for refugees. Therefore, our team presented tips for password usage to minimize these risks (Appendix G).

4.1.3 The Majority of Refugees Use Social Media for Over 3 Hours a Day

Besides the risks of people accessing refugees' personal data, challenges are presented when a refugee's LGBTIQ status is exposed such as through social media. Although social media allows refugees to communicate, access information, and learn, it puts them at a greater risk of harm (Anderson, 2018). All 13 of our surveys' respondents used social media with seven of them being on social media for more than three hours a day, and four of those seven using social media for more than five hours a day. The high volume of hours that refugees spend on social media may imply that they have become used to the technology platforms and user interface designs. It may also imply that, given enough time, they have become less cautious with these platforms than they were when they first joined. By letting their guard down, refugees are exposing themselves to needless risks. Eight respondents said they share their LGBTIQ status on social media, but only four of the respondents use an alias. The low number of aliases is concerning because twelve respondents engage with LGBTIQ content on social media, nine

respondents talk with other openly LGBTIQ individuals on social media, and seven respondents both like ("thumbs up") and post LGBTIQ content on social media. Figures 15 and 16 show more detailed responses about social media usage. Social platforms personalize content based on the individual's activity on its app. LGBTIQ refugees and asylum seekers must be extremely careful about the content they engage with because if a malicious person hacks into their account, they can see the refugee's personalized content which exposes the vulnerable individual. Because of risks like these, our team presented social media security measures (Appendix G).

Figure 15

Number of Refugees Who Interact With Social Media
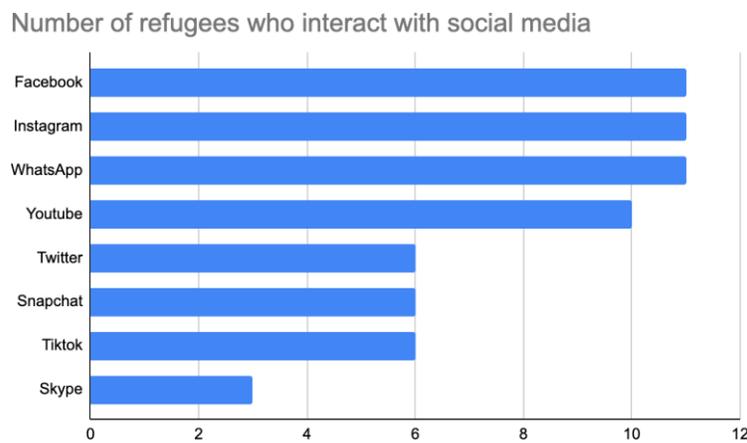
Note. Data from ORAM Refugee Survey and LGBT Asylum Task Force Survey

Figure 16

Hours a Day Refugees Use Social Media
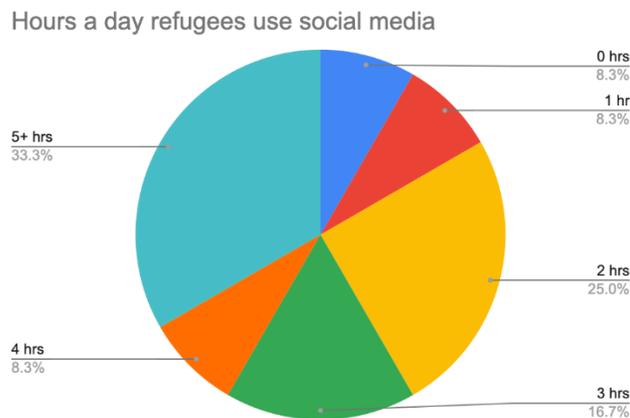
Note. Data from ORAM Refugee Survey and LGBT Asylum Task Force Survey

4.2 ORAM's Interaction With Refugees via Its Web App

Of the six respondents to the ORAM refugee survey, five answered the last part of the survey relating to ORAM's web application. With only five responses, there is a lack of data to represent a larger population. Interpreting the results from five responses can make some of the data skewed or inaccurate. When looking into the responses, our team took into account the small sample size. Out of the five, three (60%) respondents stated they were aware ORAM had a web application. The web application was created in 2020 by a WPI student team sponsored by ORAM. Having 60% of responses state that they are aware of the web application is a great basis to improve upon a year-old web application. However, all respondents had never used the web application. This may be due to the respondents previously contacting ORAM before this application was created, and therefore they have no reason to use the application. As ORAM works with more refugees and asylum seekers, we will look at how to make the web application easily accessible for those seeking help.

4.2.1 The Majority of Refugees Requested Additional Resources and Communication via Email

The last four questions in part three of the ORAM refugee survey were all short responses that pertained to the web app, contacting ORAM, and additional information ORAM can provide. The question about the web app and what features were most useful was rendered irrelevant as none of the respondents had used the web application before. However, our team recognized the need for communication. Of the five refugee respondents, two refugees requested some form of better communication via email. One respondent asked for an email address to reach ORAM. Our team analyzed these responses by focusing on ways to improve the communication side of the web application. Since email was the main response, looking into adding some type of email section was a top priority.

One of the refugees responded to the short response questions stating 'advocacy'. The response for advocacy was unclear as the respondent did not expand on it. To protect privacy, we did not collect any contact information from respondents, so our team had no way to ask for clarification. Our team took an educated guess stating that the respondent was asking for more available resources. Currently, ORAM has some informational resources in its web application.

The final two questions of the ORAM refugee survey related to what additional information or resources ORAM can provide. One of the respondents requested ORAM look into helping LGBTIQ refugees who are not staying in safe houses. The same respondent mentioned

an organization ORAM can utilize called Refugee Independence Support. ORAM has worked with Refugee Independence Support in October of 2020 to help provide work for LGBTIQ refugees. Refugee Independence Support is an organization that supports LGBTIQ refugees, specifically in Nairobi, Kenya, through providing housing and funding supplies such as food, water, and medicine (Refugee Independence Support Organization, 2021). It has a Facebook page and blog site where it keeps followers up to date on its latest activities.

4.2.2 Refugees Requested More Languages

Our survey asked respondents if they wanted ORAM to include supplemental languages in the web application and if so which ones. The current web application includes three languages: English, French, and Spanish. Out of the five respondents, 40% agreed with adding additional languages to the web app. Furthermore, one of the respondents requested that the web application include **Swahili** as one of the languages. Adding languages to the web application can be a slow process that ORAM can continuously work on, starting with adding some common languages among asylum seekers. This will provide a base of languages that ORAM can continuously expand upon.

4.3 Security and Data Collection Methods for ORAM's Application

In order to gain a more detailed understanding of the issues and concerns we are trying to address, our team conducted a series of five interviews with faculty and staff at Worcester Polytechnic Institute who have a background in cybersecurity, data protection, or information technology. The interview questions remained mostly the same for each of the interviews so that we could compare responses, but they were sometimes modified slightly depending on the interviewee's background and expertise. The general set of interview questions can be found in Appendix D.

The range of topics in these interviews was vast, but a few questions and topics came up repeatedly. Interviewees almost always asked, "who are you worried about gaining access to the information?" It became clear as we conducted more interviews that **having a good understanding of the digital threats ORAM and its users face is important before we make security recommendations**. Another thing we were advised to consider was how the data ORAM intends to collect will specifically benefit both ORAM and the refugees it helps. The overwhelming sentiment was that the **safest data is the data that is not collected**, so only ask for what is absolutely necessary and can be justified. Another common thread throughout the interviews was the idea of third-party threats. The utilization of **third-party applications or services on a website is one of the most common ways that outside groups can collect user information** and is something to be aware of when assessing threats. Finally, another frequently mentioned point was the possibility of ORAM taking on more employees to help maintain security standards and manage sensitive data storage. While these are just some of the key findings from our interviews, we also learned about data protection and cybersecurity.

4.3.1 Encryption Protects Sensitive Information

One of the most straightforward and effective ways to secure digital information is through encryption. Encryption is the process of taking a string of text or numbers and scrambling/encoding it through the use of what is known as an encryption key. In the most basic sense, encryption is a cypher that makes information meaningless to anyone who manages to obtain it. Without the encryption key, it is **nearly impossible to crack modern-day encryption**. One of the most secure and widely used encryption standards is known as the Advanced Encryption Standard (AES). AES, which was adopted by the United States government and has seen widespread use globally, includes three encryption algorithms of increasing security: AES-128, AES-192, and AES-256. Since ORAM is an international organization, the international

security standard should be taken into account, too. ISO 27000 is the international standard for how to manage information security. Most commercially available encryption services today adhere to these standards. Using an existing encryption service that adheres to ISO 27000 standards will be more than sufficient for ORAM and straightforward to implement.

Many services can be used to encrypt files in this way, all of which use at least AES-128 encryption to secure the files. On the Pro version of Microsoft Windows ($199/user), users receive access to BitLocker, which can be used to easily encrypt files (*Encryption in Microsoft 365*, 2021). VeraCrypt is free and open-source but can be slightly more difficult to use (*VeraCrypt*, 2021). Boxcryptor ($10/user/month) is easy to use with multiple users and has built-in integration with mainstream cloud services like Google Drive, OneDrive, and Dropbox (*Boxcryptor Pricing and Features*, 2021). Cryptomator is free and also integrates with mainstream cloud services but can be harder to use with multiple users (*Cryptomator*, 2021). Finally, on Microsoft Office 365 files, there is a built-in feature to easily encrypt a file with a password, and this has no additional cost for ORAM as they already use Office 365 (*Encryption in Microsoft 365*, 2021). Table 2 shows our team's analysis of each encryption service based on affordability, ease of use, and security.

Table 2

Evaluation Matrix of Encryption Services

Service	Affordability (/3)	Ease of Use (/3)	Security (/3)	Total (/9)
Office 365	3	3	3	9
Cryptomator	3	2	3	8
Boxcryptor	2	3	3	8
VeraCrypt	3	1	3	7
BitLocker	1	2	3	6

4.3.2 Cloud Storage can be used if Files are Encrypted Locally

One major takeaway from these interviews concerned the storage of sensitive data. There was a mix of opinions on the pros and cons of online versus offline databases, but the general consensus was that **if data is encrypted locally, it can be stored safely online**. Personally identifying information would certainly be safer if it was stored offline, but the risk of losing data, human error, and difficulty in accessing information from offline databases led most

interviewees to agree that an online database service is most convenient for what ORAM wants to do.

Many of the more mainstream cloud storage services, such as GSuite, OneDrive, and Dropbox, implement comparable security measures. All three of them use either AES-128 or AES-256 to encrypt files at rest, and SSL/TLS to encrypt files in transit, which is generally considered to be very secure (*Dropbox Business*, 2021; *Security, Privacy, and Cloud Compliance*, 2021; *Encryption in Microsoft 365*, 2021). Google also stores documents in different chunks, so that in order for a hacker to gain access to all of the data, they would need to do many different decryptions, as each chunk is useless by itself. ORAM could use either the free version of Google Drive, or spend $6/user/month for GSuite (*Google Workspace Pricing*, 2021). ORAM already uses Microsoft Office 365, so OneDrive would have no additional cost. Dropbox is more expensive than OneDrive and GSuite, costing $12.50/user/month. Despite all three of these services encrypting the files both at rest and during transit, they still have security vulnerabilities. When the data first arrives, it is decrypted briefly before being encrypted for storage, which provides a brief window for hackers to access the data. It also requires a certain level of trust in the cloud service because they hold all of the decryption keys to the data and can potentially decrypt and access it at any point.

Some cloud services, such as Tresorit and NordLocker, have additional security measures which fix these security flaws. They both use SSL/TLS to encrypt files in transit, but the files are encrypted with AES-256 on the user's device, using an encryption key based on the user's password (*Tresorit Pricing,* 2021; *On NordLocker File Encryption*, 2021). This means that these **cloud services never actually see the decrypted data**, nor do they have access to the decryption keys, which makes the data much safer from all threats. Tresorit costs $14.50/user/month, while NordLocker only costs $4/month (*NordLocker Plans*, 2021). Table 3 shows our team's analysis of each of these cloud storage services.

Table 3

Evaluation Matrix of Database Services

Service	Affordability (/3)	Ease of Use (/3)	Security (/3)	Total (/9)
Google Drive	3	3	2	8
OneDrive	3	3	2	8
NordLocker	2	2	3	7
Tresorit	1	2	3	6
Dropbox	1	3	2	6

We also asked interviewees what parts of data collection were at the greatest risk for being exploited by malicious groups: data collection, data transmission, or data storage. Here, the most important takeaway from the responses we received was that there should be a **comprehensive risk assessment** on all three aspects of this data collection to be sure each is secure. Appendix F shows the steps employed in the NIST 800-37 risk management framework which is used by many organizations to perform comprehensive risk assessments. Utilization of this or other similar risk management processes can help organizations be sure their data collection is secure. Malicious groups will try to exploit whatever aspect is weakest; one part is not necessarily always going to be targeted. If they are trying to gain access to information, they will utilize whatever method is at their disposal. So while it is important to secure all aspects of data collection and not leave any prone to attack, three of the professionals we interviewed agreed that the database itself would be most appealing to attackers since it has a large collection of information in one place, and if that can be accessed, then everything they would want is already in one place.

4.3.3 Strict Access Controls Increase Security

Once all of ORAM's databases are securely encrypted, the weakest link in keeping the data safe is the people who have access to the data. According to two of our interviewees, one of the primary causes of unauthorized access to data and exposure of sensitive data is not having strict enough access controls. One way to ensure that this risk is minimized is to adhere to the principle of least privilege, which says that **the only users who should have access to certain data are those who need this data to do their job** (Gegick & Barnum, 2013). It is also important to dynamically adjust who has access to the data, meaning that once a user no longer needs to use the data, their access to it should be revoked. Many of the cloud services discussed earlier have the ability to easily change who has access to given files.

4.3.4 Pseudonymization Protects Personally Identifying Information

Another way to further protect refugees' personal data that one interviewee recommended is to either pseudonymize or anonymize it. Pseudonymization is the process of replacing all of the personal data in a database with unique identifiers in such a way that only an authorized person can re-identify the data (GDPR, 2016). Similarly, anonymization is the process of changing or removing personally identifying information so that it can never be re-

identified. Both pseudonymization and anonymization are recommended for protecting personal data by the General Data Protection Regulation (GDPR), which is a regulation in EU law on data protection and privacy. Both of these processes are feasible to implement, as anonymization only requires data to be deleted, and pseudonymization can be achieved by creating a separate database that links the pseudonyms to the personal data. By applying either of these techniques, a database can afford to have less strict access controls, while further reducing the number of people who can view any personally identifying information.

4.3.5 Increased IT Support Ensures Continued Security

Finally, another common thread throughout almost all of the interviews we conducted was that ORAM should look into avenues for more IT support. Currently, they have no dedicated IT personnel and are only supported by a volunteer whose expertise is not in cybersecurity. As ORAM continues to expand its online presence, a more dedicated IT staff will become increasingly necessary to maintain the security standards required for its operations. Our security and data storage recommendations will not be a final solution for ORAM. Encryption and security standards will continue to change as hackers develop new methods, and ORAM will need to be able to update the security of its website and database to prevent malicious groups or individuals from exploiting weaknesses in its security as they emerge.

5. Conclusions and Recommendations

After analyzing responses from the LGBT Asylum Task Force and ORAM refugee surveys as well as the faculty interviews our team conducted, we identified recommendations ORAM can implement in its interactions with refugees and in its digital practices.

5.1 Recommended Security Measures for ORAM's Refugees

Our team identified three security measure categories refugees should be trained on: Wi-Fi, Passwords and Social Media. Seen in Appendix G, we created training materials that describe techniques, services, and tips LGBTIQ refugees can use to keep their personal data safe. ORAM, or any organization, can use the resources in the training materials to create informative curriculums for refugees. Our team also created an infographic, seen in Figure 17, that could appear when accessing ORAM's application so that any asylum seeker can learn about personal security measures they can adopt to keep their digital data secure.

Figure 17

Refugee Security Measures

ORAM

REFUGEE SECURITY MEASURES

Tips refugees can use to keep their personal data secure

WIFI

Verify the WiFi **network name**
○ FreeAirportWifi vs FreeairportWifi

Only visit websites with **HTTPS encryption**

Use a **VPN** (virtual private network)

Disable bluetooth when using public WiFi

PASSWORDS

Use **logical groups** to organize passwords
○ different passwords for social media and financial institutions

Use **passphrases** instead of passwords
○ "This is my super secure password 90#" can turn into TimSsP90#

Use **password managers**

Use **multi-factor authentication**

No PIN numbers, addresses, or birthdays in passwords

SOCIAL MEDIA

Don't overshare

Use an **alias**

Don't post identifying features

Avoid giving **personal information** to someone who calls, emails, or texts

5.2 Recommended Features for ORAM's Web Application

ORAM's web application needs to be made visible for people to see on its website. To do this, ORAM should make its web application a staple of its home page. Additionally, ORAM should be reaching out to the current refugees with whom they work to help promote the web application. From the responses, it is clear that some know of the web application but very few, if any at all, utilize the web application.

5.2.1 Implement Recommended Changes to ORAM's Web Application

Based on the requests we received from ORAM and our refugee survey, our team created a comprehensive list of recommended features for ORAM's web application seen in Figure 18. The contents of this infographic will be discussed below.

The web application should include some form of contact information for either ORAM to get in contact with the asylum seekers or the asylum seekers to get in contact with ORAM. The best option would be to include both. On the web application, there should be an optional field for the refugees to input their email. In addition, ORAM should have an email listed in the web app that refugees can use to contact ORAM. This gives refugees the option to personally reach out to ORAM if they feel uncomfortable sharing their email on the web application. ORAM should go no further than requesting an email from the refugees. From the interviews with IT professionals, collecting less personally identifying information is better for the safety of the asylum seekers.

Currently ORAM has an additional comments section on the web application (see Figure 9).

Figure 18

List of Recommended Features for ORAM's Web App

Recommended Features for ORAM's Web Application

1 **Languages**
Continuous addition of languages starting with popular refugee languages

2 **Email**
Refugees can reach out to ORAM's email and refugees can submit their email

3 **Resources**
Constant addition of resources including getting in contact with other organizations

4 **Number of Refugees**
Allowing a single refugee to submit a request for help for more than one refugee

5 **Country Seeking Refuge in**
Section where refugees can identify which country they are seeking refuge in

6 **Making the Web Application a Staple**
Moving the web application to make it more visible to those who use ORAM's website

Responses are not being stored from the web application. Therefore, any additional comments will not be seen by a representative at ORAM. **The additional comments section should be removed from the web application.** Once ORAM starts collecting information, there will still not be a need for the additional comments section because refugees can instead use ORAM's email to reach out to the organization. There should be a statement alongside with the email on the application saying, "For any additional help or information, feel free to reach out to us at help@oramrefugee.org." This will allow refugees to email concerns directly to ORAM instead of going through the web application.

Additionally, our team identified the need for the web application to adopt additional languages. Common languages among asylum seekers are constantly changing as different countries experience turmoil. During the years of 2008-2017, some of the most common languages among refugees were Arabic, Nepali, Somali, Sgaw Karen, Spanish, Kiswahili, Chaldean, Burmese, and Armenian (Scamman, 2018). Our team recommends that ORAM begin implementing additional language options in the web application starting with some of these. This will serve as a starting point for ORAM to expand the application's reach. More languages should be adopted as the need arises.

5.2.3 Improve ORAM's Web Application From a Mobile View

The suggestions from both ORAM and ORAM's refugees allowed our team to create a recommended design update for ORAM's web app, seen in Figure 19. We chose to illustrate these design changes from a mobile view because 68% of refugees living in urban centers have access to an internet capable phone (UNHCR, 2016). Our team added a language icon on the top left corner of the web app where users can switch to the language they desire. Next our team added questions to the web application that asked about the number of refugees seeking refuge, the country refugees are looking to seek refuge in, and a form where refugees can input their email if they desire. Lastly, we included ORAM's email at the top of the web application to allow refugees to easily contact ORAM. The line states, "Fill out this form or contact us at *help@oramrefugee.org*".

Figure 19

Recommended Design for ORAM's Web App From a Mobile View

5.3 Recommended Security Services and Protocols for ORAM

After identifying and analyzing a list of possible security measures and services that ORAM could use to better protect its data, we narrowed the list down to determine which options were most suited for ORAM's needs. We believe that the security measures described below will sufficiently protect data that ORAM collects while still remaining affordable and easy to implement. Despite the improved security offered by these measures, we still recommend that ORAM **only collect data that is necessary and can be justified, as the safest data is the data that is never collected**.

5.3.1 Protect LGBTIQ Refugees' Data by Using Encryption

Out of all the encryption services we analyzed, shown in Table 2, **the option with the best combination of security, ease of use, and price is Microsoft Office's "Encrypt with Password" feature**, which can be used to encrypt any Word, Excel, or PowerPoint file. This uses AES-256 to encrypt the entire document in Office 2016, and AES-128 to encrypt the document in Office 2007, both of which are considered to be very secure, as long as a strong password is chosen. It is also incredibly easy for ORAM to start using this feature. Existing databases can be converted from Google Sheets to Excel by clicking "File > Download > Microsoft Excel", and then Office 365 files can be encrypted by clicking "File > Info > Protect Workbook > Encrypt with Password". By implementing this, files can be safely secured in the cloud. Excel also has the option to password protect a single sheet or the whole workbook from being edited, but this does not actually encrypt the document and can be bypassed, so ORAM should ensure that it uses the encryption feature instead. **If ORAM needs to encrypt any non-Office files, then the next best option would be to use Cryptomator** which, like Microsoft Office, uses AES-256 and is free to use.

5.3.2 Safeguard LGBTIQ Refugees' Data by Utilizing Cloud Storage Services

As long as sensitive documents are encrypted locally, they can be safely stored in any mainstream cloud storage service, but based on our evaluation in Table 3 **we recommend that ORAM uses either Google Drive or Microsoft OneDrive**. Google Drive is free by default, and OneDrive comes with Microsoft Office 365, which ORAM already uses. These two services also use TLS to encrypt files in transit, and AES-256 to encrypt files at rest, which further secures the already-encrypted files. Google Drive also breaks data into chunks and stores and encrypts

each chunk in a separate location, preventing any malicious people from gaining access to all of the data at once.

5.3.3 Additional Security Recommendations

Further security recommendations we have for ORAM include:
1. Using strict access controls
2. Pseudonymizing personal data
3. Expanding its IT staff in the future

Only the people who need to view a database should have it shared with them. We suggest that ORAM **limit the number of individuals who can access the database** and the information contained in it as much as possible. Doing so will help to minimize the risk of accidentally creating gaps in security due to human error that could be exploited by malicious groups. This is especially important if the database contains personally identifying information.

An alternative to this would be to **replace any identifiable information with pseudonyms.** Then, a separate database can be created which connects each pseudonym with each refugee's personally identifying information. This second database should be encrypted with a different password than the first and should be shared with even fewer people. The information in this second database should be accessed as infrequently as possible since most work done with the information collected should be able to be carried out without the need for explicitly identifying data. For example, correspondence could still be written using an ID number instead of an individual's name.

Finally, although it is not a necessary step to take currently, **ORAM should look into increasing its IT support staff** if it intends to grow as an organization in the future. The security recommendations made here were selected with consideration towards ORAM's access to the necessary digital support. However, the field of cybersecurity is constantly evolving, and these recommendations will need to be maintained, updated, and reassessed as time goes on and new strategies for data theft are developed. We recommend that ORAM consider hiring additional IT staff in the future.

6. References

Alam, K. and Imran, S. (2015), "The digital divide and social inclusion among refugee migrants: A case in regional Australia", Information Technology & People, Vol. 28 No. 2, pp. 344-365. https://doi-org.ezpxy-web-p-u01.wpi.edu/10.1108/ITP-04-2014-0083

Al-Khal, Abdulla (2020). Gay Moroccans face blackmail, bullying after they were outed online. Thomson Reuters Foundation. https://news.trust.org/item/20200423164410-baih4/

Alfred, C. (2016). Year in Review: The Refugee Crisis in 2016. The New Humanitarian. https://deeply.thenewhumanitarian.org/refugees/articles/2016/12/29/year-in-review-the-refugee-crisis-in-2016

Alvarado, D., Gurnawan, V., De Heer, A., & Gass, B. (2020). Reducing Stigmatization of LGBT+ Refugees. Worcester Polytechnic Institute.

Anderson, S. (2018). Exploring the role of social media in the lives and well-being of young refugees in Bergen, Norway. The University of Bergen.

Asylum Procedure. (2020). Handbook Germany. https://handbookgermany.de/en/rights-laws/asylum/asylum-procedure.html#:~:text=The%20asylum%20procedure%20is%20regulated,the%20individual%20applies%20for%20asylum.

Asylum Process. (2019, July 24). Welcome Center Berlin. https://www.berlin.de/willkommenszentrum/en/arrival/asylum-process/#:~:text=Article%2016a%20of%20the%20constitution,right%20to%20protection%20in%20Germany.

Ayoub, M. (2019). Understanding Germany's response to the 2015 refugee crisis. Review of Economics & Political Science : REPS. https://doi.org/10.1108/REPS-03-2019-0024

Azizi, R. (2018). A chronology of the refugee crisis in Europe. Info Migrants. https://www.infomigrants.net/en/post/10021/a-chronology-of-the-refugee-crisis-in-europe-1

BBC News. (2018, August 30). Gay dating app Grindr to sell shares. BBC News. https://www.bbc.com/news/business-45353789

Bletscher, C. (2020). Communication Technology and Social Integration: Access and Use of Communication Technologies Among Floridian Resettled Refugees. Journal of International Migration and Integration, 21(2), 431–451. https://doi.org/10.1007/s12134-019-00661-4

Boxcryptor Pricing and Features. (2021). Boxcryptor. https://www.boxcryptor.com/pricing/

Curry, D. (2021). Dating App Revenue and Usage Statistics (2021). Business of Apps. https://www.businessofapps.com/data/dating-app-market/#2

Calka, Beata & Cahan, Bruce. (2016). Interactive map of refugee movement in Europe.

Geodesy and Cartography.65.
https://www.researchgate.net/publication/311938800_Interactive_map_of_refugee_movement_in_Europe.

Candid. (2021). *ORAM - ORGANIZATION FOR REFUGE, ASYLUM & MIGRATION*. GuideStar.
https://www.guidestar.org/profile/26-3748676

Cryptomator. (2021). Cryptomator. https://cryptomator.org/

Dropbox Business. (2021). Dropbox. https://www.dropbox.com/business/pricing

Eddy, M. (2020). The Best Free VPNs for 2021. PCMAG. https://www.pcmag.com/picks/the-best-free-vpns#:~:text=Very%20few%20VPNs%20offer%20a,offer%20totally%20free%20subscription%20levels.&text=Because%20free%20VPNs%20are%20so,to%20experience%20some%20performance%20issues.

Encryption in Microsoft 365. (2021). Microsoft. https://docs.microsoft.com/en-us/microsoft-365/compliance/encryption

Fatafta, M., & Samaro, D. (2021). Exposed and Exploited: Data Protection in the Middle East and North Africa. *Access Now*, 15-21.
https://www.accessnow.org/cms/assets/uploads/2021/01/Access-Now-MENA-data-protection-report.pdf

Fernández-Huertas Moraga, J., & Rapoport, H. (2015). Tradable Refugee-admission Quotas and EU Asylum Policy*. CESifo Economic Studies, 61(3–4), 638–672.
https://doi.org/10.1093/cesifo/ifu037

Ferrill, T. (2020). The 6 best password managers. CSO.
https://www.csoonline.com/article/3198507/the-6-best-password-managers.html

Funk, N. (2016). A spectre in Germany: Refugees, a 'welcome culture' and an 'integration politics.' *Journal of Global Ethics*, *12*, 289–299.
https://doi.org/10.1080/17449626.2016.1252785

Gegick, M., & Barnum, S. (2013, May 10). Least Privilege. *Cybersecurity & Infrastructure Security Agency*. https://us-cert.cisa.gov/bsi/articles/knowledge/principles/least-privilege

Gerhards, J.,(2016). German public opinion on admitting refugees. DIW Economic Bulletin
https://www.econstor.eu/handle/10419/141292

Gilbertson, S. (2021). The Best Password Managers to Secure Your Digital Life. Wired.
https://www.wired.com/story/best-password-managers/

Google Workspace Pricing. (2021). Google. https://workspace.google.com/pricing.html

Granados, S., Murphy, Z., Schaul, K., & Faiola, A. (2016, October 14). Fenced out. Washington Post.https://www.washingtonpost.com/graphics/world/border-barriers/europe-refugee-crisis-border-control/

Grant, D. (2015). Texts From AT&T Are Easy To Spoof. Medium. https://medium.com/@da/texts-from-at-t-are-easy-to-spoof-2b94e17bd17b

Grindr. (2019). Grindr Holistic Security Guide. https://www.grindr.com/g4e/G4E-HolisticSecurityGuide-English.pdf

Groot, J. (2021). 101 Data Protection Tips: How to Keep Your Passwords, Financial & Personal Information Safe in 2020. Digital Guardian. https://digitalguardian.com/blog/101-data-protection-tips-how-keep-your-passwords-financial-personal-information-safe

Hailbronner, K., & Thym, D. (2016, April 7). *Legal framework for entry and border controls.* https://doi.org/10.5771/9783845259208-32.

Hillstrom, L. C. (2018). UNHCR: The UN Refugee Agency. In T. Riggs & K. J. Edgar (Eds.), In Context Series. Immigration and Migration: In Context (Vol. 2, pp. 803-808). Gale. https://link.gale.com/apps/doc/CX3662200157/GIC?u=mlin_c_worpoly&sid=GIC&xid=d18ed811

Human Rights Watch. (2020). LGBT Rights. http://internap.hrw.org/features/features/lgbt_laws/

Imperva. (2021). Phishing attacks. https://www.imperva.com/learn/application-security/phishing-attack-scam/

International Rescue Committee. (2016). Afghanistan: What you need to know about one of the world's longest refugee crises. https://www.rescue.org/article/afghanistan-what-you-need-know-about-one-worlds-longest-refugee-crises#:~:text=2015%20saw%20a%20record%2011%2C000,dangerous%20country%20for%20aid%20workers.

Jancis, M. (2021). How do password managers work?. Cybernews. https://cybernews.com/best-password-managers/how-do-password-managers-work/

Jet, J. (2018). How to Stay Safe When You Use Airport WiFi. Forbes. https://www.forbes.com/sites/johnnyjet/2018/04/18/how-to-stay-safe-when-you-use-airport-wifi/?sh=245eb29d32f5

Jones, T. (2017). *Germany's Bundestag passes bill on same-sex marriage: DW: 30.06.2017.* Deutsche Welle. https://www.dw.com/en/germanys-bundestag-passes-bill-on-same-sex-marriage/a-39483785

Knight, B. (2020). Berlin builds dozens of new refugee homes despite falling numbers. DW. https://www.dw.com/en/berlin-builds-dozens-of-new-refugee-homes-despite-falling-numbers/a-53659481#:~:text=Fewer%20refugees%2C%20more%20shortages&text=According%20to%20official%20statistics%2C%20Berlin,have%20seen%201%2C575%20new%20arrivals.

LessPass. (2015). Stateless Password Manager. https://lesspass.com/#/

LGBT Asylum Task Force. (2021). Our Mission. http://www.lgbtasylum.org/home.html

License to Harm: Violence and Harassment against LGBT People and Activists in Russia. (2014). Human Rights Watch. https://www.hrw.org/report/2014/12/15/license-harm/violence-and-harassment-against-lgbt-people-and-activists-russia#_ftn103

McVane, B. (2020). PTSD in asylum-seekers: Manifestations and relevance to the asylum process. Psychiatry Research, 284, 112698–112698. https://doi.org/10.1016/j.psychres.2019.112698

Mikal, J., & Woodfield, B. (2015). Refugees, Post-Migration Stress, and Internet Use: A Qualitative Analysis of Intercultural Adjustment and Internet Use Among Iraqi and Sudanese Refugees to the United States. Qualitative Health Research, 25(10), 1319–1333. https://doi.org/10.1177/1049732315601089

Mishori, Ranit & Aleinikoff, Shoshana & Davis, Dawn. (2017). Primary Care for Refugees: Challenges and Opportunities. American family physician. 96. 112-120. https://www.researchgate.net/publication/318351440_Primary_Care_for_Refugees_Challenges_and_Opportunities

Nikendei, C., Kindermann, D., Brandenburg-Ceynowa, H., Derreza-Greeven, C., Zeyher, V., Junne, F., Friederich, H., & Bozorgmehr, K. (2019). Asylum seekers' mental health and treatment utilization in a three months follow-up study after transfer from a state registration-and reception-center in Germany. Health Policy (Amsterdam), 123(9), 864–872. https://doi.org/10.1016/j.healthpol.2019.07.008

National Institute of Standards and Technology. (2018). Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-37r2

NordLocker Plans. (2021). NordLocker. https://nordlocker.com/plans/

On NordLocker file encryption. (2021). NordLocker. https://nordlocker.com/why-nordlocker/

Organization for Refuge, Asylum & Migration. (2021). *Welcome to ORAM*. HOME-ORAM. https://oramrefugee.org/

Paletta, D. (2020, December 22). ILGA world UPDATES state-sponsored HOMOPHOBIA Report: "There's progress in times of uncertainty". https://ilga.org/ilga-world-releases-state-sponsored-homophobia-December-2020-update.

Pink News (2017, January 18). Number of LGBT asylum seekers rises sharply. https://www.pinknews.co.uk/2017/01/18/number-of-lgbt-asylum-seekers-rises-sharply/.

Refugee Council. (2020). 2014 asylum trends and facts. Refugee Council. https://www.refugeecouncil.org.uk/latest/news/4259_2014_asylum_trends_and_facts/.

Refugee Independence Support Organization. (2021). Facebook Blog. https://refugeeindependence.blogspot.com/?m=1

Rietig, V., & Müller, A. (2016). The New Reality: Germany Adapts to Its Role as a Major Migrant Magnet. Migration Policy Institute. https://www.migrationpolicy.org/article/new-reality-germany-adapts-its-role-major-migrant-magnet

Scamman, K. (2018). Refugees in the United States: Languages and Resettlement. Telelanguage. https://telelanguage.com/refugees-in-the-united-states-languages-resettlement/

Security, Privacy, and Cloud Compliance. (2021). Google. https://cloud.google.com/security

Soederberg, S. (2019). Governing Global Displacement in Austerity Urbanism: The Case of Berlin's Refugee Housing Crisis: Governing Global Displacement: Housing Refugees in Berlin. *Development and Change, 50*(4), 923–947. https://doi.org/10.1111/dech.12455

Staton, B. (2016). Eye spy: biometric aid system trials in Jordan. The New Humanitarian. https://www.thenewhumanitarian.org/analysis/2016/05/18/eye-spy-biometric-aid-system-trials-jordan

Tresorit Pricing. (2021). Tresorit. https://tresorit.com/pricing

United Nations High Commissioner for Refugees. (2000). The State of The World's Refugees 2000: Fifty Years of Humanitarian Action. UNHCR. https://www.unhcr.org/publications/sowr/4a4c754a9/state-worlds-refugees-2000-fifty-years-humanitarian-action.html

United Nations High Commissioner for Refugees. (2016). Connectivity for everyone https://www.unhcr.org/innovation/connectivity-for-everyone/

United Nations Higher Commissioner of Refugees (2016). Connecting refugees: How internet and mobile connectivity can improve refugee well-being and transform humanitarian action. UNHCR. http://www.unhcr.org/5770d43c4

United Nations High Commissioner for Refugees. (2019, April 19). Syria emergency. UNHCR. https://www.unhcr.org/syria-emergency.html

United Nations High Commissioner for Refugees. (2020a, June 18). Figures at a Glance. UNHCR. https://www.unhcr.org/en-us/figures-at-a-glance.html.

United Nations High Commissioner for Refugees. (2020b). Refugee Data Finder. UNHCR. https://www.unhcr.org/refugee-statistics/

VeraCrypt. (2021). VeraCrypt. https://www.veracrypt.fr/en/Home.html

World Bank. (2019). Population totals. World Bank. https://data.worldbank.org/indicator/SP.POP.TOTL

7. Appendix

Appendix A: Sponsor Description

ORAM was founded in 2008 by Neil Grungras. He started the company in Minneapolis, Minnesota. The organization has since expanded to have a second office in Berlin, Germany. Some notable members of its staff include Executive Director Steve Roth, Programming Director Anja Limon, Communication and Development Coordinator Bella Stevens, and Legal Program Coordinator Yeray Albelda (Organization for Refuge, Asylum & Migration, 2019). Steve Roth has an extensive background working with global organizations focused on LGBTIQ issues including education and workplace inclusion. Anja Limon has studied international law with a focus on human migration. Prior to joining ORAM, she worked for a firm in Ljubljana, Slovenia where she studied the legal gap in refugee law regarding protection for refugees affected by climate. Bella Stevens holds a master's degree in cultural anthropology and has done research focused on LGBTIQ refugees from the Middle East. Yeray Albelda has a background in theater studies and has focused his work around social justice issues. ORAM's board members include Rajiv Desai, Selisse Berry, Perry A. Witkin, and Jody Cole who serve as the board's chair, vice chair, treasurer, and secretary respectively. The work done by ORAM is primarily to serve and represent vulnerable refugees from any country of origin seeking asylum with special focus on members of sexual and gender minority groups. Since its inception, they have helped tens of thousands of people in need and are continuing to broaden its scope and reach.

Since its founding, ORAM has expanded to take on numerous programs and policies. Using a three-pronged approach, ORAM carries out across-border global advocacy (Candid, 2021). First, ORAM, a non-profit, gives refugees direct assistance by partnering with local organizations to provide services tailored to the specific needs of that LGBTIQ community. These services include refugee protection tools, capacity building, and training of adjudicators and protection professionals. Then, ORAM utilizes outreach and advocacy by working closely with governments of refugee host countries, the United Nations, international NGOs, and academic institutions to help create training programs and spread awareness about vulnerable refugees. Currently, ORAM is working on projects in numerous countries including Mexico where they have launched a legal program to assist and support LGBTIQ asylum seekers in preparing for the U.S. asylum process. For the final part of its three-step approach, ORAM conducts research to publish experiences from the exceptional lives of vulnerable refugees.

These publications have helped to pave the way for system-wide reforms. ORAM's charitable work has spread awareness about discrimination issues and has aided in empowering refugees from the grass roots upwards.

Appendix B: ORAM Refugee Survey

ORAM Refugee Survey

We are a student project team from Worcester Polytechnic Institute (Worcester, MA) sponsored by the Organization for Refuge, Asylum & Migration to determine effective security measures for their web application in order to safely collect data about LGBTIQ users.

The goal of this survey is:
(1) obtain information related to your individual experience with technology as well as your understanding of your community's experiences with those same technologies
(2) understand your level of security knowledge in topics such as data protection
(3) determine what needs of asylum seekers are not currently being met by ORAM's web app.

Your participation in this survey is completely voluntary and you may withdraw at any time. Your answers will remain anonymous; no names or identifying information will appear in this questionnaire or in any of the project reports or publications. Our project team will use this information to identify obstacles LGBTIQ refugee groups face when accessing technology as well as provide recommendations for ORAM's web application. Thank you for participating.

* Required

What is your age range? *

○ <18

○ 18-20

○ 20-25

○ 25-30

○ 30-50

○ 50+

What is your gender identity? *

○ Female

○ Male

○ Non-Binary/non-conforming

○ Prefer not to say

○ Other: _____

Describe your current living situation: (choose all that apply) *

☐ safe house

☐ apartment

☐ house

☐ camp

☐ Other: _____

Next   Page 1 of 4

Never submit passwords through Google Forms.

This content is neither created nor endorsed by Google. Report Abuse - Terms of Service - Privacy Policy

Google Forms

ORAM Refugee Survey

Your experiences with technology

Are you currently: (choose all that apply)

☐ An asylum seeker

☐ A refugee

☐ Other: _____

If applicable, what devices did you use to communicate with agencies, doctors, lawyers, or other asylum seekers during your journey?

☐ Mobile phone

☐ Desktop

☐ Laptop

☐ N/A

☐ Other: _____

If applicable, what devices did you use to communicate with agencies, doctors, lawyers, or other asylum seekers during your asylum process?

☐ Mobile phone

☐ Desktop

☐ Laptop

☐ N/A

☐ Other: _____

If applicable, did you own the device you used to communicate with agencies, doctors, lawyers, or other asylum seekers during your journey?

○ Yes

○ No

○ Some but not others

○ N/A

○ Other: _____

If applicable, did you own the device you used to communicate with agencies, doctors, lawyers, or other asylum seekers during your asylum process?

○ Yes

○ No

○ Some but not others

○ N/A

○ Other: _____

If applicable, during your journey, did you tend to use WiFi or mobile data?

○ WiFi

○ Mobile data

○ I used both pretty evenly

○ I used both but mostly WiFi

○ I used both but mostly mobile data

○ N/A

○ Other: _____

If applicable, during your asylum process, did you tend to use WiFi or mobile data?

○ WiFi

○ Mobile data

○ I used both pretty evenly

○ I used both but mostly wifi

○ I used both but mostly mobile data

○ N/A

○ Other: _____

Have you always had access to a reliable internet connection during both your journey and asylum seeking process? If not specify when you did not have a reliable internet connection.

Your answer

If applicable, during your journey, was it easy to connect to WiFi or did you rely on mobile data?

	1	2	3	4	5	
Relied on Mobile Data	○	○	○	○	○	Accesible WiFi connection

If applicable, during your asylum process, was it easy to connect to wifi or did you rely on mobile data?

	1	2	3	4	5	
Relied on Mobile Data	○	○	○	○	○	Accesible WiFi connection

To the best of your knowledge, in the community in your first country of asylum:
Applicable for next 3 questions

Internet access is readily available

	1	2	3	4	5	
Disagree	○	○	○	○	○	Agree

People have access to devices which can access the internet

	1	2	3	4	5	
Disagree	○	○	○	○	○	Agree

A majority of people own their own communication device

	1	2	3	4	5	
Disagree	○	○	○	○	○	Agree

Which way did you prefer to be contacted while you were an asylum seeker?
(Note: we will not be contacting you, this question is simply for preference purposes)

☐ Email
☐ Text
☐ Phone call
☐ Other: _____

Back   Next   Page 2 of 4

ORAM Refugee Survey

Part 2 Questions

Your knowledge of data protection

The following 4 questions have related images which will test your knowledge of common cyber security hacker tactics. Some identifying characteristics(bank names, time stamps, user names) have been edited in the images.

email #1

Would you interact with email #1? Why or why not?

Your answer

email #2

Would you interact with email #2? Why or why not?

Your answer

---

text message #1

< Messages   **658-3**   Details

Text Message
Today 8:47 PM

ATT FREE MSG: Welcome to
AT&T Mobile Locate. Click
dl.mymobilelocate.com to
complete your set-up or call
888-562-8662. Data charges
may apply.

Would you interact with this text message #1? Why or why not?

Your answer

---

text message #2

< Messages   **955-77**   Details

Text Message
Today 8:47 PM

ATT FREE MSG: Welcome to
AT&T Mobile Locate. Click
attmobilityllc.net to complete
your set-up or call
888-562-8662. Data charges
may apply. Reply HELP for help

Would you interact with this text message #2? Why or why not?

Your answer

Do you disable bluetooth when you're not using it?

○ Yes

○ No

○ Other: _____

Do you use the same password for most things?

○ Yes

○ No

○ Other: _____

If no, do you rotate between a handful of passwords depending on the site?

○ Yes

○ No

○ N/A

○ Other: _____

How to you keep track of your passwords? (Choose all that apply)

☐ Memorization

☐ Physically writing it down

☐ Electronically writing it down not in a password protected space

☐ Electronically writing it down in a password protected space

☐ Other: _____

If offered, do you use multi-factor authentication for your accounts? (password and email or text are needed to login)

○ Yes

○ No

○ Other: _____

Do you use phone numbers, addresses, birthdays, or other personally identifiable information in any of your passwords?

○ Yes

○ No

○ Other: _____

If you use some form of social media, which platforms do you engage with?
(Choose all that apply)

- [ ] Facebook
- [ ] Instagram
- [ ] Twitter
- [ ] WhatsApp
- [ ] Snapchat
- [ ] Tiktok
- [ ] Youtube
- [ ] Skype
- [ ] Discord
- [ ] I don't use social media
- [ ] Other: _____

In total, how many hours a day do you use social media?

- ( ) 0 hrs
- ( ) 1 hr
- ( ) 2 hrs
- ( ) 3 hrs
- ( ) 4 hrs
- ( ) 5+ hrs

With the content you engage with on social media, do you trust the information that is shown to you? Choose 1 if you do not use social media.

	1	2	3	4	5	
I do not trust information I see on social media	( )	( )	( )	( )	( )	I think my social media is a reliable source for information

If you use some form of social media, do you share your LGBT status on social media?

- ( ) Yes
- ( ) No
- ( ) Other: _____

If you use some form of social media, do you engage with LGBT content on social media? (Choose all that apply)

- [ ] Yes, I "like" (thumbs up) LGBT content
- [ ] Yes, I post LGBT content
- [ ] Yes, I talk with other users who openly identify as LGBT+
- [ ] No
- [ ] N/A
- [ ] Other: _____

If you use some form of social media, is your social media under an alias (fake name)?

- ( ) Yes
- ( ) No
- ( ) Other: _____

If you use some form of social media, are you ever concerned about your data being public? Why or why not?

Your answer

Do you use any dating apps? If so which ones?

Your answer

Back   Next   Page 3 of 4

Never submit passwords through Google Forms.

This content is neither created nor endorsed by Google. Report Abuse - Terms of Service - Privacy Policy

Google Forms

ORAM Refugee Survey

Part 3 Questions

ORAM's web application and what needs are currently not being met.
Here is the link to ORAM's Web App: https://oramrefugee.org/seeking-help/

Are you aware that ORAM has a web app?

○ Yes

○ No

Have you used ORAM's web app before?

○ Yes

○ No

What features or aspects of the web app do you think were the most helpful to you?

Your answer

What features would you like to see in the web app that would have helped you with the asylum process?

Your answer

Currently, ORAM's web application can be displayed in three languages. These are French, Spanish, and English. Would you want to see the web app in other languages?(If yes, please list the ones you would like below.)

Your answer

If you've ever had trouble contacting an asylum organization (like ORAM) explain why, and how they can improve?

Your answer

What additional information or services do you think ORAM could provide to help refugees seek asylum?

Your answer

Back   Submit   Page 4 of 4

Never submit passwords through Google Forms.

This content is neither created nor endorsed by Google. Report Abuse - Terms of Service - Privacy Policy

Google Forms

Appendix C: LGBT Asylum Task Force Refugee Survey

LGBT Asylum Task Force Refugee Survey

We are a student project team from Worcester Polytechnic Institute (Worcester, MA) sponsored by the Organization for Refuge, Asylum & Migration to determine effective security measures for their web application in order to safely collect data about LGBTIQ users.

The goal of this survey is:
(1) obtain information related to your individual experience with technology as well as your understanding of your community's experiences with those same technologies
(2) understand your level of security knowledge in topics such as data protection

Your participation in this survey is completely voluntary and you may withdraw at any time. Your answers will remain anonymous; no names or identifying information will appear in this questionnaire or in any of the project reports or publications. Our project team will use this information to identify obstacles LGBTIQ refugee groups face when accessing technology as well as provide recommendations for ORAM's web application. Thank you for participating.

* Required

What is your age range? *

- ◯ <18
- ◯ 18-20
- ◯ 20-25
- ◯ 25-30
- ◯ 30-50
- ◯ 50+

What is your gender identity? *

- ◯ Female
- ◯ Male
- ◯ Non-Binary/non-conforming
- ◯ Prefer not to say
- ◯ Other:

Describe your current living situation: (choose all that apply) *

- ☐ safe house
- ☐ apartment
- ☐ house
- ☐ camp
- ☐ Other:

Next Page 1 of 3

Never submit passwords through Google Forms.

This content is neither created nor endorsed by Google. Report Abuse - Terms of Service - Privacy Policy

Google Forms

LGBT Asylum Task Force Refugee Survey

Your experiences with technology

Are you currently: (choose all that apply)

☐ An asylum seeker

☐ A refugee

☐ Other: _____

If applicable, what devices did you use to communicate with agencies, doctors, lawyers, or other asylum seekers during your journey from your home country to the US?

☐ Mobile phone

☐ Desktop

☐ Laptop

☐ N/A

☐ Other: _____

If applicable, what devices did you use to communicate with agencies, doctors, lawyers, or other asylum seekers during your asylum process?

☐ Mobile phone

☐ Desktop

☐ Laptop

☐ N/A

☐ Other: _____

If applicable, did you own the device you used to communicate with agencies, doctors, lawyers, or other asylum seekers during your journey from your home country to the US?

○ Yes

○ No

○ Some but not others

○ N/A

○ Other: _____

If applicable, did you own the device you used to communicate with agencies, doctors, lawyers, or other asylum seekers during your asylum process?

○ Yes

○ No

○ Some but not others

○ N/A

○ Other: _____

If applicable, during your journey from your home country to the US, did you tend to use WiFi or mobile data?

○ WiFi

○ Mobile data

○ I used both pretty evenly

○ I used both but mostly WiFi

○ I used both but mostly mobile data

○ N/A

○ Other: _____

If applicable, during your asylum process, did you tend to use WiFi or mobile data?

○ WiFi

○ Mobile data

○ I used both pretty evenly

○ I used both but mostly wifi

○ I used both but mostly mobile data

○ N/A

○ Other: _____

Have you always had access to a reliable internet connection during both your journey from your home country to the US and asylum seeking process? If not specify when you did not have a reliable internet connection.

Your answer

If applicable, during your journey from your home country to the US, was it easy to connect to WiFi or did you rely on mobile data?

	1	2	3	4	5	
Relied on Mobile Data	○	○	○	○	○	Accesible WiFi connection

If applicable, during your asylum process, was it easy to connect to wifi or did you rely on mobile data?

	1	2	3	4	5	
Relied on Mobile Data	○	○	○	○	○	Accesible WiFi connection

To the best of your knowledge, in the community in your first country of asylum:
Applicable for next 3 questions

Internet access is readily available

	1	2	3	4	5	
Disagree	○	○	○	○	○	Agree

People have access to devices which can access the internet

	1	2	3	4	5	
Disagree	○	○	○	○	○	Agree

A majority of people own their own communication device

	1	2	3	4	5	
Disagree	○	○	○	○	○	Agree

Which way did you prefer to be contacted while you were an asylum seeker? (Note: we will not be contacting you, this question is simply for preference purposes)

☐ Email
☐ Text
☐ Phone call
☐ Other: _____

Back   Next   Page 2 of 3

LGBT Asylum Task Force Refugee Survey

Your knowledge of data protection

The following 4 questions have related images which will test your knowledge of common cyber security hacker tactics. Some identifying characteristics(bank names, time stamps, user names) have been edited in the images.

email #1

Would you interact with email #1? Why or why not?

Your answer

email #2

Would you interact with email #2? Why or why not?

Your answer

---

text message #1

< Messages   **658-3**   Details

Text Message
Today 8:47 PM

ATT FREE MSG: Welcome to
AT&T Mobile Locate. Click
dl.mymobilelocate.com to
complete your set-up or call
888-562-8662. Data charges
may apply.

Would you interact with this text message #1? Why or why not?

Your answer

---

text message #2

< Messages   **955-77**   Details

Text Message
Today 8:47 PM

ATT FREE MSG: Welcome to
AT&T Mobile Locate. Click
attmobilityllc.net to complete
your set-up or call
888-562-8662. Data charges
may apply. Reply HELP for help

Would you interact with this text message #2? Why or why not?

Your answer

Do you disable bluetooth when you're not using it?

◯ Yes

◯ No

◯ Other:

Do you use the same password for most things?

◯ Yes

◯ No

◯ Other:

If no, do you rotate between a handful of passwords depending on the site?

○ Yes

○ No

○ N/A

○ Other: _____

How to you keep track of your passwords? (Choose all that apply)

☐ Memorization

☐ Physically writing it down

☐ Electronically writing it down not in a password protected space

☐ Electronically writing it down in a password protected space

☐ Other: _____

If offered, do you use multi-factor authentication for your accounts? (password and email or text are needed to login)

○ Yes

○ No

○ Other: _____

Do you use phone numbers, addresses, birthdays, or other personally identifiable information in any of your passwords?

○ Yes

○ No

○ Other: _____

If you use some form of social media, which platforms do you engage with? (Choose all that apply)

☐ Facebook

☐ Instagram

☐ Twitter

☐ WhatsApp

☐ Snapchat

☐ Tiktok

☐ Youtube

☐ Skype

☐ Discord

☐ I don't use social media

☐ Other: _____

In total, how many hours a day do you use social media?

○ 0 hrs

○ 1 hr

○ 2 hrs

○ 3 hrs

○ 4 hrs

○ 5+ hrs

With the content you engage with on social media, do you trust the information that is shown to you? Choose 1 if you do not use social media.

	1	2	3	4	5	
I do not trust information I see on social media	○	○	○	○	○	I think my social media is a reliable source for information

If you use some form of social media, do you share your LGBT status on social media?

○ Yes

○ No

○ Other: _____

If you use some form of social media, do you engage with LGBT content on social media? (Choose all that apply)

☐ Yes, I "like" (thumbs up) LGBT content

☐ Yes, I post LGBT content

☐ Yes, I talk with other users who openly identify as LGBT+

☐ No

☐ N/A

☐ Other: _____

If you use some form of social media, is your social media under an alias (fake name)?

○ Yes

○ No

○ Other: _____

If you use some form of social media, are you ever concerned about your data being public? Why or why not?

Your answer

Do you use any dating apps? If so which ones?

Your answer

Back   Submit   ▬▬▬▬▬▬▬▬▬ Page 3 of 3

71

Appendix D: Industry Professional and WPI Faculty Interviews

We are a student project team from Worcester Polytechnic Institute (Worcester, MA) sponsored by the Organization for Refuge, Asylum & Migration (ORAM) to determine effective security measures for its web application in order to safely collect data about LGBTIQ users. ORAM currently has a web application that they intend to use to collect data such as the user's current country, country of origin, LGBTIQ status, and asylum status. It is important that this information is secure so that the vulnerable population using this app does not face increased risks. The goal of this interview is to understand what data security measures and practices may be feasible for ORAM to implement within its web app.

Introduction:
- Introduce ourselves
  - Brett, Jenna, Matt, Alex
- Explain why we want to interview them
- Provide a short summary on ORAM and its web-app. Include what it currently does and what ORAM wants it to do.
  - (We will share screen and show the current web-app)
- Talk briefly on why data protection is so important for ORAM and the people who use its services. Also mention they have one person who volunteers to do IT for them (not an extensive team).

Interview Questions:
- Can you provide us with a short background of your professional history and experience with work related to internet privacy and cybersecurity?
- What methods are generally used to track who uses a website, both by the owner of the website and by third parties
- Since ORAM is intending to start storing personal data from refugees, what methods might be feasible for this data storage? (A Google spreadsheet was utilized in the past, but we imagine this is not the most secure option.)
  - Online vs. offline
  - Would you consider it secure to store encrypted files in Google Drive or similar cloud services?
- How difficult and/or expensive might it be to transfer the information to an offline storage medium while still keeping it easily accessible and editable by ORAM employees?

- If personally identifiable information (i.e. names, emails, etc.) are not being stored, is there still a risk of sensitive information (i.e. LGBTIQ status) being connected with the person who used the web-app
- What parts of this type of data collection do you believe are at greatest risk for being exploited by malicious groups?
    - Data collection (filling out the web-app online)
    - Data transmission (sending the information to a database)
    - Data storage/access (possible risk of someone else accessing the database)
- We've done some research on ways to protect sensitive information and data encryption seems to be the most prevalent option. Do you have any knowledge on data encryption, and if so, do you know of any services that can be used for data encryption?
- We've read some sources that mention AES (Advanced Encryption Standards). While we don't know that much about AES at this time, how feasible would it be to help ORAM implement this type of encryption.

Conclusion:
- Is there anything else you see as being important to address that we may be overlooking? Or any additional topics that you think could be worth reading up on?
- Is there anyone else you know who you think it might be helpful for us to talk to?

Alternative interview questions were developed for interviewees with less IT and cybersecurity knowledge but with a background in diversity, equity, and inclusion instead.

Alternate Interview Questions:
- Can you provide us with a short background of your professional history and experience with work related to internet privacy and technology ethics?
- ORAM is intending to start storing personal data from refugees, do you believe this is worth the risk refugees might face?
- From your experience doing research on refugees in Turkey, what are the most common ways organizations may unintentionally exploit refugees?
- What ethical concerns should we be aware of when asking for information from refugees (especially if it can be used to identify the individual?)
- What risks or concerns might there still be in collecting non personally identifiable information from refugees (i.e. LGBTIQ status, country of origin, etc.)?

- What types of malicious groups do you think pose the greatest threat for targeting LGBTIQ refugees? (possible examples: governments, individual citizens, organized anti-LGBTIQ groups, international organizations)
- What parts of the data collection process do you believe have the greatest risk of exploitation by malicious groups? (data collection, transmission, and storage)

Appendix E: ORAM IT Volunteer Interview

Interview Questions for ORAM's volunteer:

We are a student project team from Worcester Polytechnic Institute (Worcester, MA) sponsored by the Organization for Refuge, Asylum & Migration (ORAM) to determine effective security measures for its web application in order to safely collect data about LGBTIQ users. The goal of this interview is to understand what data security measures and practices are currently implemented within the web app and what may be feasible for ORAM to implement in the future.

1. Can you provide us with a short background of your professional history and experience working in IT, cyber security, and with ORAM?

2. How much time do you usually devote to ORAM on a weekly basis?

3. Have any changes been made to the web app since it was created by last year's WPI group?

4. From your experience with the web app and email helpline, what do you see as being a potential security risk for ORAM? What is the way malicious groups would most likely try to exploit this data?

5. Do you know if ORAM has ever been digitally compromised?

6. Does ORAM's website/webapp utilize any 3rd parties, such as ads or third-party cookies?

7. Are there any audit logs, monitoring, or tracking on the web app?

8. What experience (if any) do you have with AES-256 encryption or any encryption standards?

9. What experience (if any) do you have with security practice standards such as ISO-27000 or NIST 800-37?

10. Around 75% of companies use Microsoft office 365 for storing info because it has plenty of security features. Do you think this would be a feasible option for ORAM?

11. What are some safe and less expensive database options you know of for storing the personally identifying data we might collect (i.e. countries where they're going to and from)?

12. Based on your experience with ORAM, do you think it would be wise for them to invest in more IT personnel to help manage and maintain higher security standards? What do you think would be the best way for them to go about expanding its investment in IT?

13. In your opinion, what improvements if any does the web app need?

14. Do you have any questions for us?

Appendix F: The Comprehensive Risk Assessment Process

1. Prepare
   a. "The purpose of the Prepare step is to carry out essential activities at the organization, mission and business process, and information system levels of the organization to help prepare the organization to manage its security and privacy risks using the Risk Management Framework." (NIST, 2018)
2. Categorize
   a. "The purpose of the Categorize step is to inform organizational risk management processes and tasks by determining the adverse impact to organizational operations and assets, individuals, other organizations, and the Nation with respect to the loss of confidentiality, integrity, and availability of organizational systems and the information processed, stored, and transmitted by those systems." (NIST, 2018)
3. Select
   a. "The purpose of the Select step is to select, tailor, and document the controls necessary to protect the information system and organization commensurate with risk to organizational operations and assets, individuals, other organizations, and the Nation." (NIST, 2018)
4. Implement
   a. "The purpose of the Implement Step is to implement the controls in the security and privacy plans for the system and for the organization and to document in a baseline configuration, the specific details of the control implementation." (NIST, 2018)
5. Assess
   a. "The purpose of the Assess step is to determine if the controls selected for implementation are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security and privacy requirements for the system and the organization." (NIST, 2018)
6. Authorize
   a. "The purpose of the Authorize step is to provide organizational accountability by requiring a senior management official to determine if the security and privacy risk (including supply chain risk) to organizational operations and assets, individuals, other organizations, or the Nation based on the operation of a system or the use of common controls, is acceptable." (NIST, 2018)
7. Monitor
   a. "The purpose of the Monitor step is to maintain an ongoing situational awareness about the security and privacy posture of the information system and the organization in support of risk management decisions." (NIST, 2018)

In this appendix, only the names of the seven steps and their purposes were provided. To read the full processes outlined under each step, see **Risk Management Framework for Information Systems and Organizations** (NIST, 2018).

Appendix G: Refugee Security Measures Training Materials

Our team surveyed refugees in contact with the Organization for Refugee, Asylum & Migration and the LGBT Asylum Task Force located in Worcester, MA to determine relevant obstacles for vulnerable populations when accessing technology. These surveys discussed refugees' individual **experience with technology** as well as their understanding of their community's experiences with those same technologies, and the participant's level of **security knowledge**. From the 13 total responses, our team identified three security measure categories refugees should be trained on: Wi-Fi, Passwords and Social Media. The following sections describe techniques, services, and tips LGBTIQ refugees can use to keep their personal data safe. This document can be used as a resource to train LGBTIQ refugees on security measures.

Asylum Seekers Should Be Cautious When Using Public Wi-Fi

Public Wi-Fi may enable malicious attacks on its users, but for refugees and asylum seekers, free Wi-Fi services are most accessible. Therefore, refugees must be wise about their Wi-Fi choice, making sure it is secure. Some steps to do this include **verifying the Wi-Fi network name** (Jet, 2018). Airports, for example, will display their Wi-Fi network in visible public spaces. When joining a network, users should make sure capitalized words and numbers are the same:

- FreeAirportWifi vs FreeairportWifi
- Airport1 vs Airport2

While connected to a public Wi-Fi network, make sure to **only visit websites with HTTPS encryption**. Although this does not make an individual's browsing completely foolproof, it does add a layer of protection when accessing their email, hotel room, or bank information. Another way to reduce one's "internet footprint" is to **use a virtual private network (VPN)**. A VPN encrypts data at the source, increasing the security of HTTP websites. Even with this added layer of security refugees still should not be transmitting sensitive information online. One downside to VPNs is their price. For example, IPVanish VPN costs $44.99 for a One-Year Plan (Eddy, 2020). Many VPNs also offer limited free versions for a month before requiring a paid upgrade which may be an option for individuals needing the service for a shorter time period. Finally, disabling Bluetooth is important when using public Wi-Fi. Eight of our survey respondents have Bluetooth enabled even when they do not use it. This simple security

measure can prevent malicious devices from connecting to someone's communication device and stealing their data.

Refugee Password Usage Needs Improvement

Passwords give access to most of our digital information which makes them extremely important to keep private. Some tips to keep passwords safe include organizing them into logical groups (Groot, 2021). For example, a person should use specific passwords for their social media but different unique passwords for financial institutions. This way if their password gets breached, not all of their information is exposed at once. Another helpful tip is to use "passphrases" instead of passwords: for example, "This is my super secure password no one will know 9 0 #" turns into TimSSpnowk90#.

It is not always feasible for someone to remember different secure passwords, especially when using logical groups and "passphrases". Therefore, **password managers are a useful tool**. A password manager is a piece of software that helps generate and store passwords in a secure location (Jancis, 2021). There are three types of password managers:

1. Locally installed password managers
2. Web-based password managers
3. Stateless password managers

Locally installed password managers are stored on a person's device and require a master password to access the offline vault of passwords. By keeping passwords offline, the only way to compromise them is by seizing the device. However, if a person wants to use their passwords on a separate device, they will need to install an online password manager which is accessible to third parties. Another downfall is that if the device is destroyed, lost, or compromised, the person will lose their vault of passwords. This type of password manager will not be feasible for refugees who own more than one device. In addition, if a refugee often shares their device with someone else there is a greater chance of their device being tampered with.

With web-based password managers, passwords are stored in the cloud. This means a person can access their passwords on any device, anywhere, at any time. The vault of passwords will be accessible for third parties to attempt to retrieve the data, but the password manager's provider encrypts all data on the device before sending it to the server. Unfortunately, most web-based password managers require payment, although some offer free versions with limited features. This type of password manager is feasible for refugees with

multiple devices and a stable internet connection because it requires an internet connection for authentication.

Stateless password managers are tools that require the site, login, and master password to generate a password. This password manager does not store the passwords in a database, but instead recalculates the password based on the 3 fields inputted into the tool which allows for automatic synchronization. Stateless password managers are also usually free and open-source which means users who do not have technical knowledge are not particularly recommended to use them because support comes from forums. Another issue with stateless password managers is that if the master password is compromised, all of the passwords are. This type of password manager has a lot of drawbacks for refugees who might have greater risks if their passwords are compromised.

1Password is a local password manager which can also act as a web-based password manager with its synchronization feature (Ferrill, 2020). 1Password is free for Windows, MacOS, iOS, and Android. A paid account is required when requesting the synchronization service. For one individual a 1Password account costs $2.99 per month with an annual commitment. There are also other plans for families and businesses and a 30-day free trial. Bitwarden is a web-based password manager that is free and open-source (Gilbertson, 2021). It does offer a paid upgrade account for $10 per year which supplies 1GB of encrypted file storage, two-factor authentication, and a password health report. However, all other features in Bitwarden can be used while still on a free account. Another option is LessPass: a free stateless password manager that is supported on iOS and Android devices, Chrome, Firefox, and even directly through a device's command line (LessPass, 2015). To address the issue of sites with specific password rules that cannot have randomly generated passwords, LessPass created a database where these complex passwords and the profile can be saved, but the password will not be saved. Depending on the individual refugee's situation, they can decide what password manager, if any, is right for them.

An additional security measure is to **use multi-factor authentication** whenever it is offered by a website or application. This means that in order to log in, a person's password and another form of identification will be required such as email or text giving their account another layer of protection from hackers. Finally, make sure no PINs, phone numbers, addresses, or other personally identifying information is being used in one's passwords. Doing so may give a hacker double the information they were expecting. By following these tips, refugees can better protect their passwords and data.

Refugees Should Not Overshare On Social Media

The participants in our refugee surveys happened to be avid users of social media. This puts them at a greater risk for digital exploitation. Our team's biggest recommendation is to not overshare on social media. Although an alias might be used, if pictures of a refugee's face or identifying features are posted with content related to the LGBTIQ community, that refugee may be actively exposing themself. Additionally, nine respondents said they talk with users who openly identify as LGBTIQ. If this individual is persecuted and their messages are revealed, it could put the refugees in contact with them in a challenging situation as well. For this reason, our team advises against giving personal information to someone who is calling, emailing, or texting these vulnerable individuals. This way refugees can avoid social engineering attacks through social media. Our team supports the expression of individuals, especially on social media, but we advise refugees and asylum seekers to beware of the content they engage with in case they must return to their country of origin.