Hi everyone, thank you for taking the time to go over this presentation with me.

I apologize for presenting out of presenter view but for some reason I could not find out how to use the software to capture a full screen view.

My name is Jason and today I will be talking about a couple of twitter employees who were charged with spying for Saudi Arabia

In case you have not know, Twitter is a microblogging system based in San Francisco, California.

It is a social media platform that became much more popular after many policymakers, politicians and celeberties use the service to casually communicate with those who are interested in hearing what they have to say.

This includes updates to laws, published papers or sometimes even just thoughts these influencers sporadically have.

Like any other social media company, Twitter requires users to provide a name, email address, and sometimes a location.

The first Twitter employee is Ahmad A-bou-ammo.

A-bou-ammo was a former twitter media manager.

In 2014 he was tasked with overseeing a majority of Saudi Arabia and was assigned with verifying a particular Saudi news journalist

This means on their twitter profile, they will now have a checkmark.

Because of his responsibility, he became with the firm’s PR, where the journalist worked, the Saudi embassy and an individual Almu-tai-ari who claimed to represent the Saudi royal family

What is so significant about the royal family, is that they are the ones with the most political power in Saudi Arabia, and are in charge of it, since it is a monarchy, unlike that of the UK and their royal family

An un-named Saudi foreign official became interested in A-bou-ammo’s position and eventually Almu-tai-ari, who was linked with this official, obtained A-bou-ammo’s email

In December 2014, A-Bou-ammo attended a Twitter conference in London, and met with this particular official and was gifted a $20,000 watch which he allegedly tried to sell on craigslist the next month

By mid-2014, A-bou-ammo used his position to gather internal records of specific politicians and celebrities, and leaked them to this foreign official

Information included emails, phone numbers, payment methods, and other personal information

One of the victims was a well known critic of the Saudi family

By May 2015, A-bou-ammo quit his position to work at Amazon, before co-founding a marketing company in the same area

According to prosecutors and the FBI, he received $100,000 via a wire transfer to an offshore bank account in Lebanon

According to A-bou-ammo he provided an invoice to FBI agents, which turned out to be fake, that he earned the money through contract work

The second twitter employee involved in spying is Ali Al-za-brah.

He was a site reliability engineer and in February of 2015 he was contacted by the same Royal Family PR, Almu-tai-ari who spoke with Al-za-brah over the phone

The two met in Washinton DC before Al-za-brah siphoned 6,000 twitter accounts half a month later

These accounts included flagged law enforcement officers and were all sent to Almu-tai-ari

One account in particular belonged to Omar Abdul-aziz who is an activist and friends with Washington Post columnist Jamal Khash-og-gi

Jamal was a well known critic of the royal family and advocated for free speech

Unfortunately in 2018 he was the target of an assassination ordered by the Saudi Crown Prince, Mohammed Sal-man

In December of 2015, Alzabrah returned to Saudi Arabia and began working with the royal family

He currently holds a B1 B2 visa but has not been back to America since

What has happened since

Both Almu-tai-ri and Alza-brah are both thought to be residing in Saudi Arabia at this time

The FBI has published these posters of the individuals

If convicted, all 3 of the suspects face 10 years and a $250,000 fine

As for A-bou-ammo, he currently faces an additional 20 years and $250,000 for destroying and altering records

Unfortunately incidents of defectors are not uncommon.

A couple examples of defecting that has happened is the Snowden incident in 2013 and more recently a Former US Air Force member defecting to Iran

According to the FBI, spies are using these social media platforms to target government contractors with security clearances

Unfortunately, some of these contractors are unknowingly speaking to these foreign intelligence officials because they use a form of social engineering to convince the contractors that they are friends for months to years on end

On a related subject, some ways governments are attempting to regulate privacy come in the form of these Acts

The first of which is the California Consumer Privacy Act that was passed and signed January 1st of this year

In summary, this act requires that companies must disclose what information they are collecting and what they are planning on using it for

Companies must comply with consumer request to delete data

Consumers are allowed to opt out of data being sold, and Bussinesses are allowed to offer financial incentives for collecting data

In addition, any California authority who knows of a breach in these terms are allowed to fine the company

Another Act that has been around is the Illinoi Biometric Information Privacy Act, similar to the ones passed in Texas and Washington state

Biometric is a way of measuring and creating a statistical analysis on an individual’s physical and behavioral characteristics.

An example is if a particular individual were to commonly search for a specific term, such as planting or yoga

These Biometrics are used to verify identity of individuals, provide security access, and sometimes assist with health plans.

This Act protects the consumer and companies must obtain consent from individuals if a company intends to collect or disclose their personal identifiers

This Act also requires that companies destroy these identifiers in a timely manner and must securely store these biometric identifiers

What makes this law unique is that it allows individuals to press charges to these companies and can come out with a nice settlement

I appreciate you taking the time to listen to this presentation and thank you for listening

I hope you have learned something new as I had.