Michael Guidry
March 30, 2017

April fools release — or a mirror of exactly how much of a joke this is not

Regression of surveillance programs worldwide

Mass surveillance is used to thwart terrorists attacks, or even find individuals for questioning regarding routine police scenarios. It could help children who may have a parent attempting to take that child out of the country beyond court orders. On the other hand it could be used to target journalists, or people who publicly comment on various topics. It is a double edged sword, and is becoming more of a problem for the average citizen as the years continue. I am not personally not against mass surveillance whatsoever. I am however going to outline some vulnerabilities, and issues that exists within these systems. It will not be a perfect system, or safer until precautions are taken into consideration on the implementations, and data being used within these systems protected. It is realistic that false positives exists today which may hurt innocent bystanders. I do not wish to go into examples but over the years there have been various news articles regarding these situations. This is a conceptual document. I have not developed any tools for exploiting these systems although I have no doubt that they work from a functional perspective. I would like you to ensure you do not break any laws but the topic needs further discussion to fix these systems before they become built into every aspect of our lives. We are at a critical point in networking technology, and with the upcoming IoT expansion it is important that these systems either get secured, or alternatives are created to replace them.

Facial recognition is an important system for finding wanted criminals, and other individuals worldwide. It may be used to stop identity theft in the near future. I am unsure as to what private intelligence companies are using it for compliance in various industries although I believe it to expand in the near future. Social security numbers are fundamentally insecure, and other systems will be required to add additional security. Banks may soon require further identification for loans, and other vast systems relating to credit. Companies are requiring Skype chats in some cases to verify identification documents. In these cases, videos may be used as evidence in later court cases.

Many other types of information is used in similar programs which are able to find structured data points within their streams to be useful for intelligence based programs. Neural networks, and other machine learning capabilities have expanded options for these data sets in recent years. It is more than likely at least half of the worlds countries are using these programs for finding individuals of interest either for monitoring, or detainment. Local city municipality, and police forces are even obtaining information for arresting individuals worldwide who may be of threatening nature to events, or cities. It relies on having data sets of individuals either from the licensing agencies for driving, or identification cards for comparison. The algorithms more than likely tie into Interpol, or national data sets as well. It depends on the nation, and their allies. It is also a leak of information to send faces of every citizen to foreign governments for comparison.

However, I am not sure whether or not everyone who uses these platforms worldwide understand the possible repercussions.

It is impossible for each individual device, camera, or city to perform these calculations which compare on their own servers locally. It means that the faces are detected within a photograph, and then extracted for submission to foreign (not local) servers or data centers for processing. It will return the results either immediately, or within a short period of time. Sometimes it may take up to 24 hours depending on the queue at that point in time. It might require a lot more processing power for a country dealing with Olympic Games to process every individual at every surveillance location such as airports. The point is that the information has to be calculated somewhere else. The data sets can be pre computed with an entire database ahead of time which would allow local processing but would leak the information, or faces of the rest of that particular category being compared against. It would mean that every wanted individual would be pre calculated so those individuals could modify their appearance until it passes the verification. It is important that these services do not ever distribute these neural network trained datasets due to this.

Neural networks are fundamentally flawed in reality. Google Deep Dream is an open source neural network application. It will insert cat, or animal photographs into a picture of your choice. It is a great example of manipulating neural networks. It reverses the situation and created random data and only uses the data if the neural network compares, and validates it. If you were to use this same type of system but with your own modifications then you can bypass neural networks which you can obtain the data sets for. If you take security products and extract their neural networks, then you have the ability to bypass these neural networks by brute forcing various factors of the information until it succeeds invisibly through these products.

Neural networks created from information generated from public data sets such as a countries citizens is flawed from the beginning. It allows manipulating, and forcing these neural networks to create false positives. The data sets would themselves become destroyed unless each individual entry of manipulation was discovered, and manually removed. It may be sorted out by date of an operation to infect the networks, although it is implausible to believe that would work alone. It would also have an entirely new issues with not being able to have an updated system without manual intervention.

Thus far terrorist attacks, and so called spies have targeted particular infrastructure, and other known publicly facing services. The issue is that everything essentially goes on the regular internet. All telecommunication infrastructures are now performing connections over the internet, and through VoIP. If you want to attack surveillance systems such as facial recognition, or platforms used for crunching information then you have to find the networks associates with it. BGP hijacking would have been a great tool, although it is tough to consider now with all of the monitoring taking place. DNS poisoning is a major possibility in a wide variety of these.

I have released a document outlining how to perform DNS poisoning with a higher window than anything currently public. Leaked malware may give some insight into the networks used. It is also possible to just DDoS entire networks of government, or other agencies while doing tests to determine if detection rates drop. Government clouds on services such as Amazon AWS is a great start. You can use your creativity to proceed with the worldwide targets. Twitter, Facebook, and other social media platforms are directed through these information gathering systems. It is easily plausible for all 3 types to be used for coordinating enough false positives to require completely new systems in place. Javascript could be used to coordinate these types of "planted information" campaigns. It could run solely on the users who agree, or within major adware networks through third party javascript.

In the past, we have all heard of students calling in bomb threats to attempt to get out of going to school on specific days. I am not condoning these actions although if you were to modify that type of motivation then you could easily learn all of the vulnerable systems, and how they interconnect to provide the security we have today. While agencies are blocking laptops from certain countries they are none smarter about real incidences which could look like normal network outages while real situations continue occurring. The fact that some of these systems also sell their services out to third parties through government associations gives the ability to directly test using their API, or as hacking targets for learning of protocols and such. I'd rather this document stay legal so I am not going to go directly into their locations, protocols, or into immediate examples. It wouldn't take more than a decent hacking group with a couple years experience to locate all of them worldwide though.

It is guaranteed that any area giving state, or national license ID cards will have some connection to upload this information to a central database. These databases are going to tie directly into the that nations allies, or Interpol. These local locations are usually less secure than others being connected to. It shouldn't be very difficult to begin locating the points of failure within these systems. It might even be easier to inject false information regarding others which may travel simultaneously using these vulnerable nodes to decrease trust in the systems overall. It is true that these systems keep past information so attempting to modify them on those massive datasets would prove difficult. If you can insert new profiles into these neural networks then you can force these neural networks to give so many false positives that they would have to be deactivated. It doesn't even have to be handled by computer hacking alone. Neural networks are created for mass verification using pre-trained datasets. If planned correctly it will be possible to just have particular people take regular IDs in an attacking fashion on a mass scale. These operations would conclude in destroying belief in the systems. A simple coordination online to help rid the world of these privacy invasive systems could cause a campaign even more destructive than other circumstances such as riots worldwide. Several thousand people in certain regions could literally cause issues to these networks where they would at least have to completely overhaul it. If the campaign becomes public knowledge then separating into various dates before, and after may help. This would be a temporary fix, and have no effect on a worldwide disruption campaign.

If you would like an example of why this would be effective then you can recognize online people have been tricking neural networks to recognize animals, and other things from patterns. It is not exactly the same but shows the precursor to these devastating attacks which essentially get data directly into worldwide neural networks without any actual computer hacking taking place. Lets consider a few thousand citizens in each country which incorporate these systems get involved and decide to trick these systems on a mass scale. If enough citizens deem these projects invasive then they could all create false positives at once thus destroying all trust in these systems. This is not something that will be fixed without a few years of overhaul especially considering the communication layer vulnerable as well.

The whole idea is that if people are tired of their privacy being invaded, then do something about it. It isn't all fun and games as people know from "Occupy Wallstreet," although these scenarios seem to be much stronger than those invidious believing camping out is going to do anything more damaging. In reality, their concepts only put more people on these lists rather than destroying the lists themselves. It wouldn't take more than a team of a few researchers to categorize the IP addresses relating to government agencies, and government "private clouds." XKeyscore, and Prism are going to come next for anyone wishing to confuse these systems. It is impossible for these systems while obtaining so much data to continue to stay private. Companies who do not agree with national security agendas more than likely aren't going to help keep their IP addresses private. It would require an entirely new algorithm, and private networking on top to keep this information to keep it safe. It is improbable that this exists except possibilities on telecommunication backbones which have many private fiber lines to various locations.

The US programs are examples because of the Snowden leaks. It is going to be the same to determine for each individual country, or Interpol associates. It will not go away until every single airport, or data collection point are on their own private connections to data centers without internet access. Disruption will come first, and then hacking will escalate once people recognize these points are "invisible vulnerabilities" to these systems. The networks keeping them private are going to be just as important as the data itself. It is highly likely that it will become a new target for "planted employees" and such. In other words, a complete restructuring of the systems will be required. This means private encryption algorithms, protocols, and service separation. It would require every single point sending data to the government cloud, or local networks will have its own connection lines outside of the internet connectable IP addresses. These attacks will be feasible for at least five years.

Let's give a quick example now. If you wanted to bypass all security in the continental United States, then you could follow a small set of steps. It might not work as easily continuously although it would definitely outline the issue, and be effective enough for a maybe a year. First you can find all government cloud providers since these are probably the services which are going to be available for all airports within America, and their allies. You could choose the particular flights you wish to allow to bypass and then

either perform DDoS attacks or significant invisible attacks on services within these networks to fill up the bandwidth they obtained. It is possible to perform other replacement attacks such as BGP, or DNS although you'd need internal information on the protocols to perform such attacks. It is much more feasible to attack all of the government clouds at once just during the landing, or take off of said individuals. This is purely conceptual by the way, and I would rather you take it as a hierarchy example of the issues with these services than a real live attack to let you bypass the restrictions. It is a simple modification of this on other networks which will let you get through other protection mechanisms worldwide.

I am unsure whether Homeland Security has any information on these vulnerabilities, or whether they have been possibly exploited in the past. I do however know that in some shape or form that everyone worldwide are vulnerable to the same attacks unless they all use private pipes. I know for a fact that it would require a lot more investment for USA networks to perform this with 90% air gapped systems on premises. It is not something that will go away, and ether they invest or fall behind the times with security.