//A PRIMER ON //SURVEILLANCE //AND INTELLIGENCE //GATHERING IN THE //CITY OF CLEVELAND

DIGITAL_FREEDOM_INITIATIVE

The Digital Freedom Initiative is a Cleveland based organization dedicated to preserving and expanding freedom, creativity and transparency in the digital world and beyond.

Contact Digital Freedom Initiative at
contact@digitalfreedominiative.org

digitalfreedominitiative.org

Cleveland, OH
2017

//CONTENTS:

EXECUTIVE SUMMARY

The purpose of this document is to overcome the gap between the understanding of the technical and political understanding of surveillance technologies and the risks they pose. To accomplish this goal we will be utilizing a threat modelling approach, or a discussion of the threats that are posed by specific technologies, and the ways that these methods inform other methods. It is only from this discussion of the capabilities, and limitations, presented with specific methods, that approaches to circumvention can be established. In this text we will review a number of tools that we believe are being used in Cleveland, or that have been used in similar contexts in other American cities in the recent past. In the discussions of these tools we will articulate the method being employed, the intent and goal of the method, the threat that is imposed by this method and the presence of local information about the use of these tools. This document is subject to revision as more information is made public.

“Under observation, we act less free, which
means we effectively are less free.”
—Edward Snowden

1.
INTRODUCTION

Throughout the past few years many of those involved in political action and protest initiatives in the city of Cleveland have come face to face with surveillance and repression. Though these overt manifestations are disturbing, and mobilized in order to generate a chilling effect on political action, these activities are only the visible aspects of a structure of surveillance that is not only increasing in the city of Cleveland, but that has come to form the core of policing nationally. As more and more information is released about these structures, a disturbing trend is becoming clear to many within the US, that the methods being employed by the police, from aerial surveillance to community policing, are fundamentally derived from tactics that were conceived of, and put into motion, during recent military occupations overseas. Much has been written about this trend toward "police militarization", but this body of literature largely ignores a fundamental fact, that the separation between police formations and the military is a purely legal, rather than functional, separation.

Since the inception of modern policing there has always been a clear connection between police and military tactics. From the development of policing out of the structures of slave patrols and the town watch groups, the police differentiated themselves from these former structures through the use of military-esque command structures, the adoption of standardized equipment and training, and even the tendency to march in column formations during their early existence, along with a tendency to hire military veterans to be police. Since this inception there has been a well documented cyclic process in which domestic police and prison control tactics have been adopted by the military, in the form of occupation and interrogation tactics, and military tactics have been adopted by the police, in the form of intelligence gathering and offensive operations.

The rise of intelligence gathering within domestic policing agencies directly mirrors the adoption of granular intelligence within military structures, and experiences the same tensions. As the amount of information about our lives expands, not only in the form of social media, but also in the form of everyday communications, the ability to gather information also expands, as do the methods of collection. This expansion of the collection of data, however, comes into contact with a limitation in the ability to process data. As information flows expand, the ability to process raw data into actionable intelligence has grown increasingly work intensive, and the pace of the expansion of information has far outpaced the growth in the capacity to process information.

Often the concern among those worried or threatened by surveillance centers around the ability to collect data, and the ways that data is collected, which should be a concern. However, with the expanding problems around processing data intelligence, gathering has shifted focus from the gathering of a significant body of data on a small number of targets to a structure in which the vast majority of resources are devoted to identifying targets from a large body of data, and then mapping the

relationships between these targets. For example, within the structure of NSA (National Security Agency) surveillance the vast majority of resources are not spent listening to calls and reading emails; there is no time for that. Rather, resources are expended collecting metadata, or the data about a communication that is not the content of the communication itself, such as phone numbers, times and dates of communication, method of communication and so on. From this data the NSA can map out whole social networks, the closeness of connections within these networks, and the correlations between communications and events.

A number of tools have been developed to facilitate this mapping of communications, and are used in concert with other tools that intercept the content of communications and methods that monitor physical activity; this is widely understood. However, the discussion around surveillance tools and methods often falls prey to two distinct problems. The first is a technical gap. With the Snowden documents the focus became on the collection of the data, not necessarily the processing and use of the data, and much of that discussion became rhetorical and technically limited. The primary reason for this is that the methods being employed by the NSA, in this case, involve highly technical processes that are not widely understood outside of technical communities. This lack of technical understanding and discourse has led to a tendency to approach these methods through the lens of political rhetoric, which may assist in slowing down the proliferation of tools of surveillance, but contributes little to understanding how they work and how they can be circumvented.

This leads to the second tendency in this discussion, a tendency to take security measures that are based on the greatest possible threat, rather than the most likely threat. We see this in the concern around the state listening to the microphones on a phone passively. This is possible, it is a threat, but for this to be the case your phone would have to have been hacked, at which point the monitoring of the microphone on your phone is the least of your worries. Also, even if you are at a meeting, and the phones are in another room, with the batteries out, the geolocation data gathered before the batteries were taken out, which shows a number of target devices in the same place, is more useful, and easier to gather, than actually listening to the microphone on the phone. Ultimately, the best defense against this specific threat, a phone compromising a meeting, is not to take the battery out but to instead leave the phone at home all together. To combat these tendencies in the discussion around surveillance takes a sober, calm and well informed discussion of the methods of surveillance, the technical aspects of surveillance and the actual threats imposed.

The purpose of this document is to attempt to overcome some of these limitations, and to open the discussion up more widely in an attempt to bridge this gap between a technical and a political understanding of surveillance technologies, and the threats that they pose. To accomplish this goal we will be utilizing a model based in the identification of the threat model, or a discussion of the threats that are posed by specific technologies, and the ways that these methods inform other methods. It is only from this discussion of the capabilities, and limitations, presented with specific methods, that approaches to circumvention can be established. In this primer we will review a number of tools that we have reason to believe are being used within the city of Cleveland, or that have been used in similar contexts in other American cities in the recent past. In the discussions of these tools we will clearly articulate the method being employed, the intent and goal of the

method, the threat that is imposed by this method and the presence of local information about the use of these tools. Readers should understand this document as a living document, one which will undergo frequent revision as more information is made public.

THREAT MODEL:

A tool of analysis which attempts to outline the risks posed by a specific threat. This approach is an attempt to fuse social and political analysis of the relation of the target to the threat and the specific risks this imposes on the target.

2.

METHOD: PASSIVE SURVEILLANCE, RELATIONSHIP MAPPING AND METADATA COLLECTION

INTENT:

To gather information widely and determine patterns in communication from large bodies of data correlated with actual events.

THREAT MODEL:

Through the release of the Snowden documents, and subsequent writing on the practice of mass metadata collection, it has become clear that the collection of data related to communications has come to eclipse more traditional forms of surveillance, such as phone taps and the analysis of content. This has occurred for two connected reasons. First, out of the engagement in Iraq, as well as experiments carried out by NSA and others in the past couple of decades, not only has it become clear that it is possible to gather mass volumes of data about communications, it has become a common argument within intelligence agencies that this is an essential function. This argument about the mass collection of data derives from a simple problem; in asymmetric conflicts, or in attempts to repress political upheaval, it is not possible to always know who the agents of these actions will be. In other words, to use a term from Donald Rumsfeld, the question shifts from one of known knowns, as in the Cold War, to unknown unknowns. As such, in order to be able to gather information on potential threats and to identify targets for more focused intelligence gathering, intelligence agencies and police have to be able to gather as much information as possible, and then use this information to identify potential targets.

The second motivating factor that has driven the rise of metadata collection is the volume of data being transmitted at any one point, which has expanded exponentially over the past decade. With this expansion, intelligence gathering bodies have run into a capacity problem. Unlike in the past, where targets would be identified through human intelligence gathering (informants) and then subjected to targeted methods like phone taps, the sheer volume of information in transit at any one time has made it more and more difficult to identify targets at all, let alone analyze this massive body of information. As such, intelligence gathering bodies have moved to a posture where they spend most of their resources gathering the data about communications, which can be automatically mapped through the use of tools, like social media monitoring platforms and the NSA's Xkeyscore system.

By focusing on metadata, intelligence analysts can spend more time on the analysis of the information being generated, and the identification of intelligence targets from this information, and less

time on listening to hours of phone calls, reading thousands of text messages and parsing millions of emails just to find a small number of actionable pieces of information. The gathering of metadata, and the use of tools to parse and organize this data shifts the focus of intelligence work from listening to communications to using communications data to draw social maps of connections, develop target profiles around the patterns of communication, and target focused intelligence more effectively against those identified as targets or nexus points within networks of targets.

Metadata collection can best be explained by the following example:

Bob calls Alice at a frequency of once per day.

Immediately after the call Alice calls another phone number which is the number of Jane, a known political radical.

This pattern repeats every day at loosely the same time.

During a recent action Bob called Alice repeatedly over the course of a couple of hours that correspond to the time of the action.

Alice then called Jane after these calls.

This is a simple example, but from this limited body of information it is possible to derive a number of possible conclusions. First, it is likely that all of these people are involved in some sort of political organizing and are working together. Second, it is likely that Bob is using Alice as a form of insulation from Jane, either for security reasons or trust reasons. Finally, given that Jane is an identified target already, it is likely that she shares commonalities politically with the other two, and that they were all involved in the political action. From this data it is then likely that Bob and Alice will be added to a list of intelligence targets.

This same pattern could be replicated with emails, text messages, Facebook posts and any number of other methods of communication, and all without knowing the content of these communications. This form of passive surveillance is widely considered to be legal, due to the absence of the need to compromise devices or the targeting of specific devices. Rather, this data is all collected, often with the assistance of telecommunications companies, who own the lines and infrastructure that is used for this communication.

From this point it becomes clear what will likely happen. The people connected to these numbers will likely be identified through their phone carriers. If they are not careful about the amount of information that exists about them on the open internet this name will become a search term that will be used to gather publicly available information on the new targets. This could include looking at social media pages, looking at any reports that have mentioned their name, finding information about schools they they have gone to and so on. In this entire process no warrants needed to be filed and no devices have had to be breached and searched. From this data it is possible to build a

relatively detailed profile of a person, their connections to others and their normal patterns of life.

The process could be repeated with any other form of passive information gathering. The gathering of geolocation data for devices has been used in the past to connect possible targets to one another and to certain events. Police in Cleveland have been known to put police cars with license plate readers outside of rallies and political events to scan license plates. In other cities it has become possible to use facial recognition cameras to passively collect data about who is in a space at any given time, and what frequency they are in that space without watching the footage live or processing videos later; though this technology is experimental. Other means that could be employed, but there is no evidence of current deployment, would be monitoring traffic on public wireless networks that a possible target could be in at a given moment, such as city or neighborhood open wifi networks or networks in a coffee shop or restaurant.

For these methods to yield actionable intelligence, however, a number of conditions need to be present. First, there has to be a pattern that can be picked out of a wider body of data, that is anomalous enough to be identifiable. This could include a consistency of calls between certain numbers, the attempt of a device at an IP address attempting to access a service at another IP address on some identifiable schedule, or the correlation of communications around certain events. Second, there has to be some reason for this pattern to be correlated to activity threatening to the state, such as a protest or other political action, events at known subversive spaces or communications within a known subversive website, communications protocol or organization. Finally, for this information to be actionable this data needs to be tied to a specific person or identity. Metadata is depersonalized, it reveals nothing about a physical person, just their patterns of life. As such, the potential target needs to provide information, such as a phone registration, social media account, internet presence, vehicle registration, etc, that allows the intelligence gathering body to move beyond the simple revelation of a connection between devices and a pattern of communications.

The collection of passive information is often augmented by the collection of data on the open internet, both through social media sites and through a simple use of the world's greatest information index, Google. It is almost cliché to say that social media itself is the greatest intelligence gathering tool that has ever been created. The primary problem is that, cliché aside, this statement could be said to be true. Social media sites are filled with the personal details of our lives, from the much maligned pictures of one's stylish breakfast to a clear articulation of networks of friends, family and passing acquaintances. We put our entire lives out there for display, willingly, and openly, allowing details to be passively collected, both by the companies running the services, and literally anyone else with an account or the money to purchase access to social media monitoring tools. The ubiquitousness of social media in our lives has generated a situation in which many political organizers conduct their business openly on Facebook, or some other clear text service, like discussion forums or chat sites. This leads to an obvious risk, not only in divulging organizing details, but also in just exposing those that may be involved in organizing itself.

As with the proliferation of data in general, the rise of social media has generated a similar problem for intelligence bodies, the pace at which data is expanding is far outpacing the ability to gath-

er and analyze the data. Many of these intelligence bodies, as well as many private corporations have begun to turn to social media monitoring services, which are alternately marketed as tools to manage public image or tools to identify potential future risk. These services use scripts to tap into the raw data streams of social media sites through APIs (Application Program Interfaces), allowing them to pull in large amounts of data automatically. This data is then made searchable through a web interface that organizations pay to access. These tools allow for the monitoring of specific accounts, the ability to search for keywords and the ability to monitor for mentions of a specific brand or institution on social media platforms.

LOCAL USE:

Information on the gathering of metadata by Cleveland police is sparse and circumstantial. No specific internal documents have been released publicly at this point to either confirm or deny the existence of a program like this. What we do know is that relationship mapping tactics have been utilized in the recent bust of the Heartless Felons and a number of other street gangs. Relationship mapping was also used recently by security at Beachwood Place to respond to a possible mass fight that was being organized for the mall. In both of these cases the primary medium for information gathering was social media sites, and it is unclear whether this is part of a larger and more automated program.

It is also clear that relationship mapping has been used to map the relationships between activists. This was clear in the lead up to the Republican National Convention, where activists and radicals were targeted for door knocks, workplace visits and phone calls demanding information both about protests for the convention, as well as information about other organizers, radicals and activists. It has also been recently revealed that in the wake of the arrests at the demonstrations against the Inauguration in Washington DC the district attorney has sent a subpoena to Facebook for location tracking and relationship information in relation to two defendants. This pattern of activity seems to indicate at least the presence of a form of relationship mapping, but again, not necessarily the use of bulk metadata collection.

What we do know is that federal agencies, including the FBI, will collect metadata from telecommunications companies and online service providers, as well as third party online service providers, like Google, through the use of National Security Letters. It is also known that this information is routinely used for federal investigations, many of which are carried out for the purposes of intelligence gathering, rather than prosecution. This information is also routinely passed to local law enforcement agencies and other governmental agencies through Fusion Centers, one of which, The Northeast Ohio Regional Fusion Center, is in Cleveland.

3.

METHOD: SURVEILLANCE CAMERAS

INTENT:

To gain visibility into public space and generate a visible deterrent effect.

THREAT MODEL:

Cameras have become ubiquitous in everyday life in recent years, and the distinctions between public and private camera systems has largely broken down in practice, even if the distinctions legally exist. This has presented a number of problems that we will be discussing in this section. The use of cameras is intended to overcome a simple series of problems that are present in on the ground policing. For policing to be universally effective it has to be universally present, or in other words, for the law to function everywhere the police have to be present to impose law everywhere, all the time. Now, this is clearly impossible, due to logistical limitations and concerns around civil liberties and authoritarianism. As a result of the limitations of the presence of police forces, combined with the reduction in the cost of camera systems, hard drive storage and networking equipment, as well as federal grant programs, police department all around the US have begun to construct elaborate camera systems, each with its own eccentricities.

Traditionally, before cameras began to proliferate, camera systems were largely divided into public camera systems, which were owned by cities, subject to Constitutional limitations and public records law, and private systems, which were limited in scope, primarily focused on capturing images of private space, and outside of Constitutional limitations and public records law, but within the civil legal system. In the past number of years this distinction has begun to break down. In New York, Cleveland, Chicago and other large cities private cameras are being tapped into the public camera system, with the footage begin sent to central viewing locations. This system has been augmented by the creation of databases of private cameras, further expanding the reach of camera systems into everyday life.

These systems have tended to be a combination of two different methodologies. The first methodology is one that is based in deterrence, in which the cameras are visible and clearly marked. These cameras serve the role of presenting the possibility that action is being watched, in an attempt to subtly modify behavior to fit with established legal norms. This is being combined with a growing array of non-visible cameras which serve the purpose of gathering evidence to increase rates of incarceration. Initially camera systems were primarily used to track down suspects in violent felonies, but increasingly they are being used to police lifestyle crimes, minor misdemeanors and to gather intelligence on targets for purposes other than prosecution.

As with metadata collection programs cameras are being used to map out movements, follow the activities of specific individuals and watch patterns of life within certain areas of a city. In a recent press conference that the Cuyahoga County Prosecutor's Office did with the Detroit Shoreway Neighborhood Development Organization they discussed the use of private centralized camera systems, combined with public cameras and license plate readers to track the movements of any possible suspect anywhere in the city from point A to point B. We will discuss the Detroit Shoreway camera system in a little bit, but structures like this begin to completely erode the division between public and private camera systems while maintaining the legal division. In other words, increasingly private cameras are being mounted in public space—Cleveland is a pioneer in this arena—and these cameras exist outside of normal Fourth Amendment limitations, as well as public records law.

This increasing privatization of the cameras and footage itself is being combined with the outsourcing of the running of surveillance programs to private corporations and the use of public-private partnerships to construct public systems. This not only privatizes the cost of the building of camera systems, allowing the systems to proliferate ever more widely, but also muddies the legal waters in such a way that new, and never before seen, configurations of cameras, in different forms, with different concepts of ownership are popping up all the time. But, with this proliferation a problem arises. As with any form of communication it becomes more and more difficult to analyze the data as the volume of data increases. This has led many police departments to resort to a combination of large scale cloud storage of footage, in order to retroactively watch footage after an event, as well as to investigate the use of facial recognition technology and predictive technologies that are meant to collect focused data about a space, even if no one is watching (these systems are, at this point, unreliable and experimental).

What this results in is a space in which concealing one's identity for a limited period of time, during a march for example, only has limited effect, unless one has already scouted the area and knows, with certainty, that the areas that they will use to exit the area are either outside of camera range or in a space that is obscured from view. As we have seen in the past series of years camera footage has been used by police to arrest participants in political actions after the action has ended, sometimes weeks later. It has also been used to follow the movements of organizers, conduct surveillance on spaces in which meetings are occurring, and gather information on people present in a given space at a given time. This means that the threat of cameras are not only present during a certain activity, in the recording of immediate activities, but remains present in the routes that one uses to leave an action, on the street one lives on, which may be under watch, and in the movements one takes everyday. As such, circumvention is only possible if one is both careful about movements, as well as conscious of the positioning of cameras in the area.

LOCAL USE:

Locally the camera systems are broken up into three distinct systems, privately owned cameras, cameras within the CS3 (Cleveland Shared Security Surveillance) camera system and cameras that

are privately owned but accessible by law enforcement. The CS3 system was initially conceived of in 2007, as a system of wirelessly connected cameras in a test system around Public Square. Since that time it has ballooned to a system of over 120 cameras before the Republican National Convention (RNC), combined with an unknown number that were installed in the lead up to the convention, which are owned by the city, as well as an unknown number of privately owned cameras that are tapped into dispatch. This system now stretches into most neighborhoods that border Downtown, and is starting to expand into other neighborhoods, like Detroit Shoreway, Clark Fulton and others. Within this system footage is sent to routing stations and recording servers, where it is archived, as well as sent to central dispatch. It is also possible for the police to park a command vehicle in the area and receive live streams of all of the connected cameras within range. There is not currently a comprehensive map of the locations of all of the cameras in the city that is readily available, but this is being assembled by some local organizations.

This system exists along side of another camera system being assembled by the Prosecutor's Office. In its initial existence the system was nothing other than a database of privately owned cameras that were registered online by owners committed to giving footage to police. However, from this beginning point the program has grown, and taken on a form very much different than its initial structure. This past fall residents of the Detroit Shoreway neighborhood became aware of a security camera program being constructed by the Detroit Shoreway Neighborhood Development Organization (DSCDO), which aimed to construct a camera system, owned and operated by DSCDO, and comprised of over 200 cameras, that was capable of having line of sight surveillance capability down a large number of residential streets. As residents began to ask questions about the system another reality became clear. Not only was the system owned and operated by the local development corporation, but each grouping of cameras would be remotely accessible by the police at any moment.

Further, residents also learned that this was connected to an initiative by the Prosecutor's Office to encourage the construction of a large number of these sorts of systems by private entities all around Cleveland in an attempt to build a camera system that has the same concentration of cameras as New York City, one of the most heavily filmed cities on Earth. This entire system, due to its private ownership, would exist completely outside of settled Constitutional law, and completely outside of public records standards, with all access being hidden from the public. Even more disturbing, the intention was to have the police decide where the cameras would be placed. This is specifically threatening to residents of the Ecovillage, an area in the Detroit-Shoreway neighborhood, many of whom have faced direct surveillance by police, door knocks by local and federal officials and even helicopters hovering over their streets during demonstrations, all due to political organizing activity.

The intention of the Prosecutor's Office system is to build a camera concentration so dense that it would be possible to combine camera footage with any number of other intelligence sources, including license plate readers, IMSI catcher data and physical surveillance to gather not only information of the movements of any person within the city, but also to comprehensively gather information on specified targets. This capability, once constructed and organized, would not only

allow the state to follow and monitor the movements of targets throughout the city, but would also allow them to gather information about targets over long periods of time which, once combined with other forms of intelligence, not only assists in gathering information that cannot be intercepted through communications channels, such as one on one discussions, as well as more effectively mark and target individuals for arrest.

4.

METHOD: PHYSICAL PROXIMITY SURVEILLANCE (STAKEOUTS, STALKING, DOOR KNOCKS AND INTIMIDATION)

INTENT:

Targeted information gathering and intimidation.

THREAT MODEL:

When many people think about intelligence gathering they tend to think of physical proximity surveillance; the team of cops in the car with a camera, the surveillance team perched in the building across the street with binoculars and so on. The reality is that this form of surveillance is becoming less and less common, and there is a good reason for this; it is incredibly work and resource intensive. To perform physical surveillance, for the purpose of gathering actionable information, takes a whole team a large number of hours, often monotonous hours, watching for the slightest sign of anything that they may be interested in. During this time the intelligence team is often within visible range of a situationally aware target, increasing the possibility of exposure. There are often easier means to gather information.

What has come to replace physical proximity surveillance has been metadata collection, social media monitoring and infiltration techniques, which can often be conducted either by a small number of agents and/or can be largely organized at a distance. With the amount of data that we put out into the world it is significantly easier to, in most cases, allow the target to expose the data themselves in public, and if they hide behind a wall of privacy settings, to create a fake account and friend the target on any number of platforms.

As such, the use of physical proximity tactics has changed shape, from methods that attempted to gather information, to methods that are largely aimed at focused targeting of persons of interest through entrapment and subversion, and the use of tactics of direct contact to generate an intimidation effect. The first of these appropriations, the use of physical proximity operations in order to engage in infiltration and subversion, has gained favor in intelligence communities. Over the past decade long term undercover agents were exposed in numerous cases involving the activist community as well as innumerable cases that have targeted the Muslim community. In many of these cases the agent was undercover for a year or more, was given a house and an income, and used relationship development and trust building as their primary tactic, and often the agents are reused for other operations in other cities. These operations were initially undertaken to infiltrate an organization to gather information that was not publicly available, identify

potential targets and then entrap those targets by developing a relationship, often financial, with the target.

In other cases tactics much more like those outlined in the US military documents around the use of local forces in counterinsurgency operations have been used. In these cases sympathetic local forces, or forces that are willing to be sympathetic if given benefits, are used to both divide political initiatives, by creating a narrative of good activists and bad radicals, as well as to gather information on those involved. This can take the form of the use of moderate elements , which are given permits and a seat at the table, to delegitimize and gather information on more radical elements. This can also take the form, as we saw with the Peacekeepers' Alliance (which we will discuss more later) of having organizations which are outside of the political initiatives be used to infiltrate organizations and actions for the police, or otherwise be used as informal police during actions. Other appropriations of this tactic involve the use of snitches, members of a group that they can convince to either provide information or engage in an operation to capture or entrap other members.

In its other guise the use of physical proximity surveillance is meant to generate a sense of intimidation and fear. This takes the form of activities as simple as leaving FBI business cards in someone's door, knocking on doors with armed police and calling organizer's phones in an attempt to "ask some questions". From there these tactics will escalate to visible stakeouts of houses, which are meant to be seen, following organizers home from meetings or actions, or asking people that are connected to a target questions about the target, knowing that this will be reported back to the target. At its most extreme this will escalate to the form of house raids, surreptitious entries into buildings (what are called Sneak and Peek searches) and the issuing of subpoenas for grand jury investigations. These tactics are all meant to generate a sense that a target is being watched, which either forces them to slow down activity, lose trust in those around them or increase security protocols, which tend to slow down activity and limit the reach of activity if done incorrectly.

A more subtle form of physical proximity surveillance comes in the form of community policing. Within this framework the goal is to utilize police-community relations bodies to bring the police into ever aspect of everyday life within a community, and to position the police as both a necessary stakeholder in all decisions as well as to develop relationships with residents that will be leveraged for intelligence gathering. These relationships, and the organizations of sympathetic residents that are created, are then tasked with providing information on elements of the community that may be engaged in either illegal activity, or "threatening" activity, a term vague enough to encompass political activity that is deemed unacceptable by the police themselves. Following its development out of counterinsurgency theory, community policing approaches then use this information on "troubled elements" to target focused surveillance, intimidation operations or direct police action.

LOCAL USE:

These tactics are a standby of both the Cleveland Police and the local FBI field office. Throughout the movement against police violence there were numerous reports of activists being followed

home from meetings, specifically meetings held at the bookstore Guide to Kulchur. People within the collective around the bookstore reported police parked outside of their homes, sometimes for hours or days at a time. During demonstrations undercover police would walk around the outside of crowds attempting to identify "leaders" and helicopters would hover over streets in the Ecovillage, where a number of organizers live. This tactic of intimidation was escalated in the lead up to the RNC, where dozens of organizers and local radicals reported FBI, local police and Sheriff's Deputies showing up at their houses or places of work, to "just ask some questions" about activities around the RNC and to identify people that were in contact with members of specific organizations. This became so common that the door knocks and intimidation became a national news story, with outlets like the Intercept writing long articles about the activity, and a number of other news organizations sending crews into Cleveland to interview organizers, many of which would only speak anonymously.

The degree to which the local police are willing to employ tactics of intimidation is nothing new to those that have been active in the community for some time. These forms of intimidation and subversion were prevalent during the early 2000s, during the antiwar movement, play a significant role in the history of political organizing on the East Side during the COINTELPRO years, and even stretch back to the early 20th Century where police here utilized the same tactics against anarchists, trade union organizing committees and the Civil Rights Movement.

The local FBI regional office has turned infiltration and intimidation into an art form. During Occupy they were working with an informant by the name of Shaquille Azir, a local man who had joined the Nation of Islam during a stint in prison, and who was facing charges for passing bad checks. They initially sent him in to spy on radical organizations on the East Side, with a specific goal of targeting Muslim organizations. After not making much headway there they turned his focus to anarchists around Occupy, and sent him to spy on the eviction of Occupy Cleveland, specifically looking to develop relationships with anyone that was wearing a mask. During that engagement he met a group of 5 participants, and began to develop a relationship with a number of them. From these relationships he became the landlord for the group, their employer and began to supply them with alcohol, cigarettes and sometimes illicit substances. This all led to him threatening their employment and housing in order to talk them into going along with a bomb plot that ended up with their arrest and federal incarceration. Azir is still active within Cleveland, participating in an operation to entrap the owner of a former observatory in East Cleveland for illegal scrapping. During this time he had been arrested, while on parole, and had his charges quietly dropped.

This sort of infiltration is just the tip of a much deeper iceberg. During the lead up to the Brelo verdict the City of Cleveland supported an expansion of the Cleveland Peacemakers' Alliance, along with a number of local nonprofits and foundations, to equip the organization to play a disruption and intelligence gathering role in coordination with the police. Information gathered on this organization, and its participants, demonstrates that not only were some of them being directly tasked with infiltrating marches and meetings by the police, specifically in Second District, but at least one member, Angel Arroyo (the Ward 6 Councilman in Lorain), bragged about being sent to Ferguson and New York City to spy on organizers, and was seen in a picture coming out of the

FBI Regional Office on Lakeside. During marches they were tasked with controlling the crowds, even up to attempting to prevent marchers from going down roads that the police did not want disrupted, and were in direct communication with the police. Not only was this group being used to gather intelligence on organizers and groups, they were also being paid, indirectly, by the City of Cleveland, with the money being funneled through nonprofit organizations run by former Cleveland Brown's wide receiver Reggie Rucker, a scandal which only came to light after Rucker embezzled over $100,000 of the money to pay for gambling debts; he is now in federal prison.

Talking to organizers that have been active in Cleveland will yield any number of other stories of attempted infiltration, harassment and disruption by both local police and federal agencies. There is a very long history of these tactics in the city, and this reality creates a profound chilling effect, not only on attempts to organize within the city, but on even the simple act of expressing displeasure in public forums. For as troubling as this is, it is nothing compared to the use of these tactics within normal everyday life in the city. Not only are sting operations and infiltration operations continuously going on, some of which are hinted at in news stories, but there are innumerable stories of people in the city who are targeted by the police heavily for simply being classified as troubled elements, including youth of color. Physical proximity surveillance and intimidation, though not the most effective means of gathering information, has become an everyday reality for many of the residents of Cleveland, often in the form of intimidation, operations which are spoken of by the city as deterrence or intervention operations. Combined with the rise of community policing with Cleveland, and the development of resident groups dedicated to aiding the police in information gathering, physical proximity surveillance has left the confines of the official police, through a clear attempt to use the community itself as a tool of police intelligence gathering and the disruption of social and political groups.

5.

METHOD: IMSI CATCHERS (STINGRAYS)

INTENT:

To intercept and monitor content of cellular device communications, the location of users or cut service entirely to a localized area.

THREAT MODEL:

There are few devices and tools used in surveillance that have generated the same amount of fear, misunderstanding and concern as the use of IMSI catchers, colloquially known by the Harris Corporation branding of the devices as Stingrays. There have been volumes of news articles written about Stingrays, numerous investigations have been launched, long form investigative pieces have been written, and even with all of this work there is still little understanding of the use and deployment of these devices by local police and federal agencies. Of the data that has been collected there are some specific conclusions that can be drawn with a level of certainty that we would like to review here.

The use of Stingrays and their technical features vary somewhat between devices and manufacturers, but they all operate in roughly the same way. At their core an IMSI catcher is a device that sets up a mobile base station for GSM, or cellular, communications. As a cellular device user moves through any space their device is constantly sending beacons out to towers around the area, and connecting to the tower that has the strongest signal. When a device connects to a tower it conducts a simple “handshake”, it requests a base station identification from the base station, and in return sends it an IMEI number, or a unique device identification number. After this exchange a connection is established and the base station begins to route communications.

All a Stingray is, at its core, is a mobile base station, which can be easily operated by non-technical personnel. When turned on all cellular devices in the area will connect to the new, malicious base station, and will begin to route communications through this device. This attack, referred to as a man in the middle attack, allows the attacker, in this case the police or federal officials, to monitor the location of devices based on their IMEI number and intercept communications.

To monitor the location of a target cellular phone user the police have already likely gathered intelligence about this user, and obtained either the IMEI number of a known user from their cellular carrier, or obtained a name to attach to a known IMEI number. This information, combined with the strength of the connection to the phone would allow police to pinpoint the location of a known target relatively accurately. In situations in which this is used for general monitoring, such as a

demonstration context, the device can be used to monitor the locations of devices with specific IMEI numbers, either to track the movements of groups of people, or merely to gather information to be used in investigations later. In this mode of simply relaying communications to legitimate towers it is unlikely that the user would notice any change in their service.

If the monitoring capability of the device is turned on, and the police begin to actively monitor communications, then they have to perform what is known as a downgrade attack on the communications. When a device makes a handshake with a base station the base station is able to choose a method through which communications may be encrypted. This means that by sitting in the middle of the connection between the device and a legitimate base station the IMSI catcher can convince the cellular device to use no encryption when it is connected to the IMSI catcher. Then the IMSI catcher will forward the communication on to the legitimate base station using an encryption protocol determined by the legitimate base station when the IMSI catcher connects to this legitimate station. By inducing the device to not encrypt its messages the IMSI catcher is able to read messages and listen to calls in plain text. Protocols like Signal, which encrypt text messages and calls separately from the negotiated protocol between the device and the base station, can be an effective means to mitigate this threat in this deployment.

Contrary to reported sightings of IMSI catchers, and photos circulating on social media, the IMSI catcher does not require a large antenna, and is not a device that is mounted on top of a vehicle. Rather, IMSI catchers are rather small, often consisting of a simple metal box with switches on it and a laptop. In the vast majority of cases the IMSI catcher can fit on top of the passenger seat of a squad car, but are often too big to be carried by a single person. This means that, unless one is keeping very careful track of the base stations that they are connected to, and monitoring for abnormally sudden changes, it is unlikely that one will even notice that an IMSI catcher is deployed in the area.

There are a number of rumored, and even documented, capabilities of some IMSI catcher systems, which have not been confirmed by any documentation or court records. This includes functionality to downgrade all connections from 4G to 2G, which is an unencrypted, non-data protocol. By downgrading the connections the IMSI catcher is able to prevent the use of tools like Signal, which utilizes a data connection, rather than voice or text, to operate. Another rumored capability of at least some systems is that they can just refuse to pass calls or communications on at all, essentially blocking cellular communication in an area. Again, these capabilities are rumored to have been deployed and are technologically possible, but there is no verification of their existence.

In some discussions of Stingray systems there have been other capabilities that have been rumored to exist, even though there is no evidence of their existence, and little technical basis to assume that they actually function. Primary among these rumors is the rumor that police can hack a phone using an IMSI catcher. Without getting into technical detail, in all of the tests that have been conducted by security researchers around systems that mimic the same functionality of IMSI catchers, no one has been able to successfully send exploits or remotely compromise a phone through the use of an IMSI catcher. There are other ways to compromise cellular devices that have

been used by police and intelligence agencies, and we will discuss these later, but these do not involve IMSI catchers, and often involve malicious text messages or emails.

The reason rumors can proliferate around IMSI catchers so easily is that there is little information about the specifics of the devices that are currently for sale on the open market. What we do know is that the first patent for an IMSI catcher was filed by Rohde & Schwartz in 2003 in England. There is significant evidence that these devices were deployed during the Iraq War extensively, and then made their way into American and British police departments. From there their use has exploded, and almost every large police department in the US, and many small and medium sized departments, are rumored to have purchased the devices. During the purchase of these devices companies such as Harris Corporation often force customers to sign non-disclosure agreements, which prevent the agency from providing information about the use of the device. In some jurisdictions this has led prosecutors to drop cases when IMSI catcher data and deployment is required as part of discovery in criminal cases.

The complete lack of any form of transparency that typifies the use and deployment of IMSI catchers has led to discussion which is either short of details or populated by speculation, which is often not grounded in technical research. This has generated a discourse that is full of claims that are often unable to be supported, and a significant amount of inaccurate information, much of which leads to ineffective approaches at circumventing or addressing the threat. From the research that has been conducted we do know that IMSI catchers can intercept calls and text messages, and we know that they can track the locations of individuals. We are unsure whether they are capable of downgrading the cellular protocols used to connect to a base station, or whether they can shut off cellular service. At this time the control of the proliferation of IMSI catchers has been such that none have been able to reach the private research community. With this being the case some security researchers have taken to using open source software and technical equipment to mimic the functionality of IMSI catchers in controlled laboratory environments. In these conditions of uncertainty it is important to limit speculation, and to take common sense counter-measures (such as leaving a phone at home during a demonstration, or using a burner phone) to limit possible effects of the deployment of IMSI catchers.

LOCAL USE:

On the question of local use of IMSI catchers the short answer is, we have no idea. Given the recent Republican National Convention, coupled with the proliferation of these devices among major city police departments, it is reasonable to assume that if the Cleveland Police did not have IMSI catcher before the convention, then they likely have them now. However, as far as our research into the question, we cannot find any mentions of their use in criminal trials, we cannot find any reference in any public documents, and we cannot find any records of their purchase.

In a recent research project undertaken by the ACLU on the purchase and deployment of IMSI catchers there was no obtainable information of their use not only for Cleveland, but for the entire

state of Ohio. This means that we are left with nothing other than assumption and the rumors of their use. It is safe to assume, however, that they have been deployed at various times, for various reasons, and given the tendency toward Cleveland being used as a testing ground for new surveillance technology and systems, it is likely that they are being used not infrequently, at least in criminal cases. Therefore, it is safe to assume that for those that fear being a target of these devices that taking reasonable counter-measures (using Signal to encrypt calls and text messages for example) is a justifiable action to take at this time.

6.

METHOD: DIGITAL DEVICE INTRUSION

INTENT:

To gain and maintain persistent information gathering capabilities on a device owned or controlled by a target.

THREAT MODEL:

Day after day news of state-sponsored computer hacking has come to dominate the news cycle. When combined with the proliferation of online fraud, malicious email campaigns and large scale data breaches, the general perception is that the internet has become a necessary, but treacherous place. Most of these stories, however, center on the use of computer hacking by foreign powers, with China and now Russia coming to dominate the coverage of computer hacking. What is discussed less, outside of the technical press, is the use of similar techniques by the federal government and local police, often in collusion with information security companies, like Hacking Team, an Italian company that is known to have sold intrusion software to not only US government agencies, but also intelligence agencies around the world.

As with the use of IMSI catchers we only see brief glimpses into this world, often when some detail of an operation becomes public through court proceedings. Beside the mass dumping of data on NSA operations, often carried out through their Tailored Access Operations Unit, there is little awareness of the proliferation of what the FBI refers to as Network Investigative Techniques, or the legally approved hacking of target machines. This has begun to change, first with the discussion around the use of malware to identify users of Tor Hidden Services, as well as the recent controversy around Rule 41.

The first case surrounds the use of malware to identify users of Tor Hidden Services. The Tor network is an anonymity network that, when coupled with the use of Tor Browser, utilizes a communication protocol that routes internet connections through an network of routing servers, obscuring the location of the user. A Tor Hidden Service is a service that is being hosted within the network which hides both the IP address of the user of the service and the service itself. In this specific case it became known, through discovery in a criminal case around the FBI investigation into a child porography site that the FBI utilized an exploit in Tor Browser, discovered by researchers at Carnegie Mellon University, to install malware on the computers of users of the site, and then use this malware to track the location of the users, which led to warrants for their arrest.

It is important to note that just as on the open internet, some abhorrent things are hosted on Tor

Hidden Services, but these are widely used by activists and journalists to circumvent repression and maintain anonymity. To conduct this operation the FBI seized the site and then ran the site for three weeks from their own servers, essentially making the US government the world's largest distributor of child pornography for that period of time. During that time they had infected all of the images on the site, and constructed them to run an exploit on any computer that downloaded the image, leading to the computer downloading malware which exposed the location to the FBI. For months the FBI resisted providing information to the court about the existence and use of this specific exploit in this case, arguing that if the exploit were known then the team around Tor Browser would patch the vulnerability, effectively preventing the FBI from being able to compromise the computers of the users of targeted Hidden Services. After a number of appeals being filed the courts demanded that the FBI release the method of exploitation, but not necessarily the code, although this is still being debated.

The second case, around Rule 41 of the Federal Rules of Criminal Procedure, derives from a Supreme Court ruling around the use of warrants to hack target devices by the federal government. Based on the complications on a case in Texas, where the FBI used a warrant issued by a judge in another Federal Court District to justify the hacking of a computer, the Advisory Committee on Criminal Rules for the Judicial Conference of the United States created a proposal, which was passed to the Supreme Court, and then to Congress, which would dramatically expand the ability of federal agents to hack computers. In proposing the amendment to Rule 41 of the Federal Rules of Criminal Procedure, the Supreme Court gave Congress till December 1st to reject the proposal, or it would be entered as an amendment to Rule 41, which governs procedures around Search and Seizure. Congress refused to take any action, and Rule 41 has been officially entered into law. The amendment clarifies the rules around warrants for computer intrusion, allowing any federal agent to obtain any warrant from any federal judge in any jurisdiction for the ability to hack any computer in the world as part of an investigation.

Outside of federal law enforcement then powers of police to either force entry into digital devices, or compel arrestees to provide passwords for devices is increasing every day. This is coupled with the recent revelations around the purchase of the Cellebrite Universal Forensic Extraction Device (UFED) by a large numbers of police departments around the country. This device contains exploits used to gain access to a large number of phones, and is capable of copying the content of an attached device through a simple point and click, or touchscreen, interface. There have also been cases in which computers have been seized without the knowledge of the operators of the systems, as in a case in which the FBI walked into a datacenter that hosted some servers for riseup.net, took one of the servers off of the server rack, attempted to copy the hard drive (and failed due to the full disk encryption Riseup Collective uses on all their servers) and then returned the server to its former location.

These intrusions have also extended outside of the attempt to utilize exploits to break into computers and seize phones, but extend to the use of malicious emails and text messages to target mobile phones. Though there are few cases of this being leveraged in the United States directly, around the world governments are beginning to utilize methods to break into the phones of dissidents

remotely. Using frameworks purchased from private companies, such as Hacking Team, government agents can easily assemble malicious messages, send them to targets, and maintain consistent access to the device. This allows them to monitor communications, install further software, steal contacts and even take pictures with the camera or listen to the microphone. As we mentioned earlier, in the introduction, the concern around government agents listening to the microphones on cellular phones would require this level of catastrophic compromise.

With the expansion of government powers to hack computers there are some common sense precautions that can be taken, and these work on a gradient from less to more complex, less to more secure. The best method of security is to prevent the device from becoming targeted in the first place. This could involve taking actions that range from using Tor Browser for much of your daily browsing activity all the way to using Tails, a free, open source, privacy centric operating system. It is also important to patch your systems whenever possible, to prevent vulnerabilities from being easily exploited. It is also important to set strong and unique passwords for all of your accounts. This means using a password manager that you have on your own computer, like Keepass, and not one that is hosted on a cloud service, like LastPass.

The most simple and clear advice is to not open up messages and attachments from senders that you do not know or messages that you did not expect. With the hacking of the DNC the attackers compromised the computer of a staffer by sending them a malicious email, which is by far the most common means of infection. From the access that they obtained they then logged in to the Gmail account of this staffer and sent everyone in their address book an email that indicated that there may have been a breach at the DNC, and that everyone should click on a specific link and change their password. When they clicked on the link they got infected as well, and the attackers moved from there. From this access they were able to move freely within the networks of the DNC, and connected networks, taking whatever data they wanted. So, even if the message comes from someone you know, if you are not expecting it then call them first and ask if they sent it.

From here the methods utilized can become more and more detailed and could include running Linux, rather than Windows or OS X. If one wants to really focus on security, while still maintaining the ability to communicate, this could involve utilizing different devices for different forms of communication with different groups and so on. Overall, there is no such thing as a perfectly secure system, and there is no such thing as perfect security. The key is to maintain the ability to continue to communicate while taking the precautions that are necessary for the level of risk and exposure one is comfortable with. A number of organizations, such as the Electronic Frontier Foundation and Riseup provide well written and non-technical guides for privacy online and information about the growth of online repression and government sponsored computer intrusion.

LOCAL USE:

On a local level there is little to no information about the use of either computer intrusion techniques or the use of UFED devices by the Cleveland Police. However, what is known is that before the RNC

some members of the Cleveland Police did undergo a computer intrusion and forensics training, paid for with federal security grant dollars. It is also known that the Ohio State Highway Patrol purchased a number of UFED devices in 2011, and that they were active in operations around the RNC.

It has long been known that the NSA routinely carries out computer intrusion operations, some of which are rumored to have been conducted within the US on non-citizens. It is also known, after the cases in recent months, that the FBI has used, and now has increasing power to use, computer intrusion techniques. Given that fact that they have purchased computer intrusion software from Hacking Team, compelled researchers at Carnegie Mellon to give them exploits for Tor Browser and have been arguing intently for their ability to expand hacking operations, this practice is likely to continue and expand.

Therefore, it is important for every organizer, activist, radical, journalist, attorney and people just concerned with their privacy to take information security seriously. At its most basic information security based countermeasures can be as simple as updating your system when updates are released, running a good antivirus, like Windows Defender or Avast, and not opening messages that either come unexpectedly or from senders that you do not recognize. If you want to take it further then it is crucial to do some research, get information from trusted sources, like the Electronic Frontier Foundation, and not fall prey to the hype cycle that often surrounds discussions of government hacking operations. Hacking computers is not magic, and the federal government, outside of the NSA, is not even particularly good at it. Most of the ways that intrusions occur center around the use of malicious messages and common exploits. As such, employing a little care and intention to how you communicate and interact online, the software you download and run on your system (and where you are downloading it from) and patching known vulnerabilities when updates are available will provide a significant, but not bullet-proof, improvement in one's security.

7.
CONCLUSION

The primary take away from all of this information is both simple and complex; we know that the state is engaging in wide scale surveillance, and that this is becoming more and more a part of everyday life, but we have little information as to the specifics of these operations. We also know that the discussion around surveillance, partially due to a lack of verifiable information and partially due to the technical aspects of the discussion, tends to be dominated by conjecture, fear and apprehension. It is also the case that the discussion that does exist within technical communities tends to exist at a separation from the everyday user, and is based in a process of research and the development of tools that is confined to a small, highly technical, group of hackers, security researchers and digital radicals that often meet to discuss these questions at obscure computer security conferences. Though these barriers exist to a rational understanding of the threats that are posed by different tactics of state surveillance, with a bit of information, some training and workshops, the development of tools that are easily used and also secure and clearly articulated expressions of both the threats posed and the needs of those at risk, a discussion can develop which overcomes these limitations.

The city of Cleveland has always been a place in which grand social experiments have been conducted. From the building of the Museum of Art and the early 20th Century structuring of the city around a paternalistic and arrogant millionaire class through the experimental housing projects of the pre-war years and into the modern era of policing and surveillance experiments, we have always been in a unique position to see trends before they expand outside of the city itself. Over the past series of years the Cleveland Police, in concert with the FBI and sympathetic local nonprofit organizations, have built a surveillance apparatus that permeates into many aspects of everyday life, from our movements around the streets to our neighborhoods, from the trip to the grocery store to our attendance at political rallies. This system incorporates a wide variety of techniques to gather, process and correlate information in order to develop a clear understanding of elements that the police interpret to be threats.

In some ways what we are seeing in Cleveland is an expansion of past methods. But, at the same time, we are also witnessing the development of a constantly expanding security state, the incorporation of new methods of surveillance, like relationship mapping, and the use of older methods, like door knocks and physical surveillance, being appropriated for different strategic goals. These modifications are partially a result of a changing social and political landscape, partially the result of the funding opened up in the era of the security state, and partially the result of methods that have been developed in foreign theaters of war and occupation.

In this primer we have been able to just touch on the basic elements of surveillance operations within the city of Cleveland, and some methodologies employed by federal agencies that are active

in the city. There is a lot more information out there, both of a technical nature and a structural nature, that we did not have time to touch on in this document, or that we are unaware of the existence of. With the prospect of the attempt to build privatized public surveillance systems throughout the city, the expansion of the city controlled surveillance network and the deployment of informal police forces, in the form of the Peacemakers' Alliance and compliant residents within community policing structures, we are facing a vast and rapid expansion of surveillance beyond the already intrusive bounds that formerly existed.

In light of this expansion of surveillance into everyday life it is important for anyone that is active in any activity that may be deemed threatening by the police to think clearly about the ways that they can protect and secure their ability to speak and act. Information security is never a process of finding the perfect solution to all forms of intrusion and surveillance. Technologies change, and so do the methods used to counteract these technologies. To maintain safety in the face of a growing surveillance apparatus means to be informed about what is going on around you, to research the ways that others have dealt with these problems, and to make decisions about how one is going to communicate based on this understanding. With the security state expanding every day the considerations around communication, and communication itself, has become something central to political action and our everyday lives, and we have to approach it as such.

digitalfreedominitiative.org